SCC

SCAP Compliance Checker
Version 5.0.1
for Windows

.

Developed by:
Space and Naval Warfare (SPAWAR) Systems Center Atlantic
P.O. Box 190022
North Charleston, SC 29419-9022
ssc_lant-scc@navy.mil

Table of Contents

1. INTRODUCTION

The Security Content Automation Protocol (SCAP) Compliance Checker (SCC) is a SCAP 1.2 Validated Authenticated Configuration Scanner, with support for SCAP versions 1.0 and 1.1, and an Open Vulnerability Assessment Language (OVAL) adopter, capable of performing compliance verification using SCAP content, and authenticated vulnerability scanning using OVAL content.

1.1 Background

1.1.1 About this Manual

This User Manual is intended to explain all of the features and functionality of the SCC application, along with some basic information regarding the SCAP standards. As SCC is used by thousands of people across hundreds of government agencies, a single Standard Operating Procedure (SOP) is not feasible. Each agency may need to create their own SOP based on their intended usage of SCC.

For DOD Usage, and integration with the Security Technical Implementation Guides (STIG) Viewer, please refer to DISA's (Defense Information Systems Agency) documentation, which is located at:

http://iase.disa.mil/stigs/Pages/stig-viewing-guidance.aspx

1.1.2 What is SCC?

SCC is a SCAP 1.2 Validated scanner but also supports SCAP 1.0 and 1.1 and SCC is an OVAL interpreter. At its core, SCC is an XML interpreter of SCAP content, meaning SCC does not perform any checks without SCAP/OVAL XML content. The end user can install SCAP content into SCC, and enable one or more SCAP content streams to perform compliance checking.

1.1.3 What is SCAP and SCAP Content?

At a very high level, SCAP is a set of XML standards, primarily XCCDF and OVAL, which include policy settings and technical instructions to perform automated checking.

SCAP Content is a collection of XML files, usually bundled in a zip file, which defines the checks to be evaluated on a target system or targeted systems. This bundle, or 'stream', instructs what checks to perform, provides all text fields such as titles, references, descriptions, and to some extent, how to perform them. SCAP validated scanners such as SCC ingest the stream and perform the checks listed therein.

The SCC application has some SCAP content pre-bundled with it from DISA and NIST (National Institute of Standards and Technology). However, SPAWAR, does not own nor maintain the content, it is only included for end user convenience. This content will need to be manually replaced periodically by the user, when content authors publish updates.

1.2 Platforms Supported

- Microsoft Windows 7 (x86 & x64)
- Microsoft Windows 8 (x86 & x64)
- Microsoft Windows 8.1 (x86 & x64)
- Microsoft Windows 10 (x86 & x64)
- Microsoft Windows Server 2008 (x86 & x64)
- Microsoft Windows Server 2008 R2 (x64)
- Microsoft Windows Server 2012 (x64)
- Microsoft Windows Server 2012 R2 (x64)
- Microsoft Windows Server 2016 (x64)
- Microsoft SQL Server 2000/2005/2008/2008R2/2012/2014
- Cisco IOS 12.x
- Cisco IOS 15.x

Note 1: *There are separate SCC installers per architecture (Windows, Linux (RPM, DEB), Solaris, Mac, AIX, HP-UX) and cross platform scanning is not supported.*

Note 2: *'Supported' is defined as the application has been designed to run on the Operating System and architecture, and has been tested in our lab to execute as expected. Content may not be provided, but end users could obtain content from other sources, or write their own, and install and run in the application. See below for the list of content included in the installer.*

1.3 SCAP Content Included

1.3.1 SCAP Streams

DISA STIG content obtained from: http://iase.disa.mil/stigs/scap/Pages/index.aspx

- DISA STIG SCAP Benchmarks
  - Adobe Acrobat Reader DC Classic
  - Adobe Acrobat Reader DC Continuous
  - Google Chrome
  - Internet Explorer 11
  - Microsoft .NET Framework
  - Windows Defender AV
  - Windows Firewall
  - Microsoft Office 2010
  - Microsoft Office 2013
  - Microsoft Office 2016
  - Windows 2008 Member Server
  - Windows 2008 Domain Controller
  - Windows 2008 R2 Member Server
  - Windows 2008 R2 Domain Controller
  - Windows 2012 and 2012 R2 Domain Controller
  - Windows 2012 and 2012 R2 Member Server
  - Windows Server 2016
  - Windows 7
  - Windows 8 and 8.1

    - Windows 10
- NIST USGCB Windows Content Release Date 2015.04.20
    - Windows 7 Operating Systems
    - Windows 7 Energy
    - Windows 7 Firewall

1.4 Changelog for 5.0.1

Below is an abbreviated list of the primary changes from version 5.0 to 5.0.1. Please refer to the release notes for a complete list of updates.

- For All Platforms
  - Fixed bug with deviations
  - Made improvements to SCAP 1.2 Tailoring functionality
  - Fixed issues with Cisco IOS support from GUI
- For Windows
  - Fixed bug with certain file searching scenarios
  - Changed file searching method to cache search results for a scan session, which may improve overall performance, depending on number of searches in content
  - Fixed minor issues with windows ntuser probe not reporting on non-existent keys
  - Improved registry probe efficiency with pattern matching

1.5 Changelog for 5.0

Below is an abbreviated list of the primary changes from version 4.2 to 5.0. Please refer to the release notes for a complete list of updates.

- For All Platforms
  - New graphical user interface
  - Added command-line and graphical method for setting all content to a single profile
- For Windows
  - Improved support for checking IIS servers with appcmd
  - Improved support for Windows Server 2016 and Windows 10
  - Fixed issues reading NTuser.dat files for certain registry content
  - Removed official support for Windows Vista
  - Fixed issue reading certain 32 bit Windows registry keys
  - Integrated Optional "Service Configuration Editor" into the options menu
  - Improved remote WMI error handling
  - Updated default remote scanning mode to WMI method

2. REQUIREMENTS

2.1 Minimum Hardware/OS Requirements

SCC can run on virtually any Windows based computer, however, below are some minimum specifications.

HARDWARE	MINIMUM/RECOMMENDED
CPU	Intel/AMD x86 or x64 based processor. Recommend at least a 1.5 Ghz dual core or newer.
RAM	1.0 GB Minimum, 2.0 GB or more is recommended. SCC uses about 250 MB to startup, and may use up to 1 GB or more during certain scans, especially WMI based remote scans from 64 bit Windows.
Disk space installation	The base install of SCC requires approximately 150 MB of disk space. Reviews may generate 100+ MB of results depending on content and logging options enabled.
Operating System	Windows 2008 or later

2.2 Scanning Requirements

SCC has three scanning modes for Windows. Local, Classic Remote and WMI Remote. Each have slightly different requirements.

SCANNING REQUIREMENT	LOCAL	CLASSIC REMOTE	WMI REMOTE
Local Administrative Rights	X	X	X
Manage Auditing and Security Logon User Right	X	X	X
Windows Management Instrumentation (WMI) Service	X	X	X
Domain Admin Rights		X	X
File and Printer Sharing for Microsoft Networks		X	X
Server Service		X	X
Firewall Exceptions ○ *If the client firewall is blocking WAN/LAN connectivity to the file shares or WMI, SCC will not be able to perform a remote review. Classic reviews also require firewall rules to allow Remote Registry access, and DCOM.*		X	X
Remote Registry Service		X	
DCOM (if content which uses WuaUpdateSearcher)		X	
Ability to execute Windows 'makecab.exe'			X

3. INSTALL/UNINSTALL

To obtain a copy of the SCAP Compliance Checker software please refer to the Technical Support section of this manual.

3.1 Windows Software Installation

Note: Installer should be run with an Administrator account.

3.1.1 Graphical Installation Method

1. Double click on the installer (SCC_5.0.1_Setup.exe).
2. Read the License Agreement page, click "I accept the agreement", and click Next.
3. Choose the Destination Folder (or leave at the default) and click Next.
4. Select Components (or leave default)
    a. Determine if pre-bundled SCAP content from NIST and/or DISA is desired.
    b. Determine if installing as a service is desired. Refer to the section titled 'Running SCC as a Service' for additional information.
5. Select a desktop shortcut if desired
6. Read the Ready to Install page and click Install.

3.1.2 Command Line Installation Method

The Setup program accepts optional command line parameters. These can be useful to system administrators, and to other programs calling the Setup program.

`/HELP, /?`
Shows a summary of this information. Ignored if the UseSetupLdr [Setup] section directive was set to no.

`/SP-`
Disables the 'This will install... Do you wish to continue?' prompt at the beginning of Setup.

`/SILENT, /VERYSILENT`
Instructs Setup to be silent or very silent. When Setup is silent the wizard and the background window are not displayed but the installation progress window is. When a setup is very silent this installation progress window is not displayed. Everything else is normal so for example error messages during installation are displayed and the startup prompt is (if you haven't disabled it with DisableStartupPrompt or the '/SP-' command line option explained above).

`/SUPPRESSMSGBOXES`
Instructs Setup to suppress message boxes. Only has an effect when combined with '/SILENT' or '/VERYSILENT'.
The default response in situations where there's a choice is:
Yes in a 'Keep newer file?' situation.
No in a 'File exists, confirm overwrite.' situation.
Abort in Abort/Retry situations.
Cancel in Retry/Cancel situations.

Yes (=continue) in a DiskSpaceWarning/DirExists/DirDoesntExist/NoUninstallWarning/ExitSetupMessage/ConfirmUninstall situation.
Yes (=restart) in a FinishedRestartMessage/UninstalledAndNeedsRestart situation.

5 message boxes are not suppressible:
The About Setup message box.
The Exit Setup? message box.
The FileNotInDir2 message box displayed when Setup requires a new disk to be inserted and the disk was not found.
Any (error) message box displayed before Setup (or Uninstall) could read the command line parameters.
Any message box displayed by [Code] support function MsgBox.

`/DIR="x:\dirname"`

Overrides the default directory name displayed on the Select Destination Location wizard page. A fully qualified pathname must be specified. May include an "expand:" prefix which instructs Setup to expand any constants in the name. For example: '/DIR=expand:{pf}\My Program'.

`/TYPE=type name`

Overrides the default setup type. Options are Standard and Custom, selecting Custom is required to select components as listed below

`/COMPONENTS="comma separated list of component names"`

Overrides the default component settings. Using this command line parameter causes Setup to automatically select a custom type. If no custom type is defined, this parameter is ignored.
Only the specified components will be selected; the rest will be deselected.
If a component name is prefixed with a "*" character, any child components will be selected as well (except for those that include the dontinheritcheck flag). If a component name is prefixed with a "!" character, the component will be deselected.

The available components are:

```
Content\NIST_USGCB_SCAP_Content
Content\DISA_STIG_SCAP_Content
Other\SCC_Service
Other\SCC_Config_Editor
```

This parameter does not change the state of components that include the fixed flag.

Example:
Deselect all components, then select the "SCC Service" and "SCC Config Editor" components:

```
/COMPONENTS="Other\SCC_Service,Other\SCC_Config_Editor"
```

Examples

Install SCC with default options silently with no GUI shown

```
SCC_5.0.1_Windows_Setup.exe /VERYSILENT
```

Install SCC to a given directory with default options silently with no GUI shown

```
SCC_5.0.1_Windows_Setup.exe /VERYSILENT /DIR="C:\SCC"
```

Install SCC with the Service and Config Editor with default content silently with no GUI shown

```
SCC_5.0.1_Windows_Setup.exe /VERYSILENT /TYPE=custom
/COMPONENTS="Content\NIST_USGCB_SCAP_Content,Content\DISA_ST
IG_SCAP_Content,Other\SCC_Service,Other\SCC_Config_Editor"
```

3.2 Windows Software Uninstall

3.2.1 Standard Method

1. Click Start -> Programs -> SCAP Compliance Checker 5.0.1 -> Uninstall.
2. Read the Welcome Screen and click Next.
3. Read the list of Files not Deleted and determine if the files should be deleted or kept. By default, the uninstaller does not remove any file created after the installation.
4. Click Finish.

3.2.2 Silent Uninstall

To perform an automated, silent uninstallation, run the uninstaller via command line with a /SILENT or /VERYSILENT flag

```
"C:\Program Files\SCAP Compliance Checker 5.0.1"\unins000.exe
/SILENT
```

3.3 Install/Remove software via zip file

3.12.1 'Install' software via tar gzip file

To install, simply extract to any directory.

Note: *Due to the amount of data that could be generated, and sensitive nature of the data, only install to an appropriate partition/directory.*

3.12.2 Removal of software installed via zip file

To remove software 'installed' from the generic zip file, simply remove the installation directory and all sub-directories and files.

3.3 Install Details

3.3.1 Files Installed by the SCC

FILE	DESCRIPTION
cscc.exe	Launcher program for the command line version of SCC
cscc32.exe	32 bit version of SCC, must be executed from cscc.exe, not directly from cscc32.exe
cscc64.exe	64 bit version of CSCC, must be executed from cscc.exe, not directly from cscc64.exe
scc.exe	Launcher program for the graphical version of SCC
scc32.exe	32 bit version of SCC, must be executed from scc.exe, not directly from scc32.exe
scc64.exe	64 bit version of SCC, must be executed from scc.exe, not directly from scc32.exe
options.xml	Default options file used by SCC
hosts.txt	Sample host file
unins000.exe	Uninstaller for this application
Documentation\ReleaseNotes.txt	Summary of changes for this version of the software.
Documentation\SCC_Help.chm	Compiled, searchable help file
Documentation\SCC_UserManual.pdf	PDF version of the User Manual
Documentation\TermsOfUse.txt	Text file containing the Usage, which is displayed during the installation.
Resources\Compiled*	Folder containing compiled library files for SCC use
Resources\Content*	Parent content folder for SCAP, SCAP 1.2, OVAL, OVAL External Variables, and OCIL content folders
Resources\Content\External_Variables	Contains any External Variables files associated with an OVAL content stream
Resources\Content\OVAL_Content	Contains any OVAL vulnerability content included with the installer or installed by the end user with the Install OVAL Content feature.
Resources\Content\OCIL_Content	Contains any stand alone OCIL content included with the installer or installed by the end user with the Install OCIL Content feature.
Resources\Content\SCAP_Content	Contains any SCAP 1.0 or SCAP 1.1 content included with the installer or installed by the end user
Resources\Content\SCAP12_Content	Contains any SCAP 1.2 content included with the installer or installed by the end user
Resources\Content\TrustedPublicCerts	Contains known/trusted certificates to verify digital signatures in SCAP 1.2 content
Resources\Content\XCCDF_Tailoring	Contains XCCDF Tailoring files which can be used with SCAP 1.2 datastreams

Resources\DB	Database utilized when processing SCAP 1.2 data streams
Resources\DefaultFiles	Contains default files used by the SCC
Resources\Deviations*.xml	Contains any user created deviations
Resources\Graphics*	Images and icons used with SCC.exe
Resources\Schema*	Files used to validate the SCAP XML content
Resources\Thresholds*.xml	Contains the default and any user customized compliance thresholds
Resources\Transforms*	Files used to create post scan HTML and text reports from the OVAL and XCCDF XML results
Temp	Location in which SCC writes temporary files during execution.
C:\Users\All Users\Microsoft\Windows\Start Menu\Programs\SCAP Compliance Checker 5.0.1	Start menu icons created during the installation process

3.3.2 Registry Keys Created During SCC Installation

REGISTRY KEY	DESCRIPTION
HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall\SCAP Compliance Checker 5.0.1	Standard uninstall information which allows the Add/Remove Programs to remove the SCAP Compliance Checker software.

3.3.3 Files Created During Software Execution

FILE	DESCRIPTION
<User Defined Directory>\Results Refer to Data Directory option in "Editing Options" for details.	XML, HTML and Text based results created during a review
<User Defined Directory>\Logs Refer to Data Directory option in "Editing Options" for details.	Screen, Error and Debug logs that could be created during a review depending on user preferences.
<User Defined Directory>\options.xml	Configuration settings from the SCC.exe
<SCC Install>\Temp	Temporary files created during SCC execution

4. GUI BASED USAGE

Section 4 of this document explains the basic Graphical User Interface (GUI) usage of SCC to perform SCAP based compliance scanning, standalone OVAL and OCIL scanning, and editing options.

Below is a quick overview of how SCC works.

1. Open the SCC GUI.
2. View available SCAP content included with SCC.
3. Install any additional SCAP content into SCC.
4. Enable SCAP content and select the desired profile from each SCAP content stream.
5. Scan Computer(s) with enabled SCAP content.
6. View reports.

4.1 Launching the Graphical User Interface

To start the application with a GUI, click:

Start -> All Programs -> SCAP Compliance Checker 5.0.1 -> SCAP Compliance Checker (SCC) 5.0.1

4.2 Installing & Configuring Content

SCC's installer contains the latest publicly available SCAP content from DISA and NIST, which was available at that time. However, new and updated content may need to be installed by end users, especially if the current SCC release is several months old.

4.2.1 Installing Content

The steps below will guide you through installing content within SCC. Note that the steps are the same SCAP 1.0, 1.1, and 1.2 data streams. To obtain DISA STIG SCAP content, please download "benchmarks" from http://iase.disa.mil/stigs/scap/Pages/index.aspx

1. Launch the SCC GUI
2. Content should be visible by default in the main window. If content is not visible, due to existing scan logs, click the "Show Content" button in the left column, "Select Content" pane.
3. Click on the "Install" button in the "Content" pane
   a. Select from the following options:
      i. Validate XML on content install (Yes/No)
      ii. Overwrite existing content (Yes/No)
      iii. Enable content on install (Yes/No)
4. Browse to the zip file containing a single content stream, or a zip of content streams of the same type such as:

   - Zip of all SCAP 1.0/1.1 files
   - Zip of all SCAP 1.2 files
   - Zip of all standalone OVAL files (not part of a SCAP stream)
   - Zip of all standalone OCIL files (not part of a SCAP stream)
   - Mixing of content types (SCAP/SCAP1.2/OVAL/OCIL) is not supported

5. After installation is complete, enable the content and choose the desired profile.

4.2.1.1 Note on DISA STIG "Manual"

DISA STIG "Manual" files are not SCAP content. They contain an XCCDF XML file, but do not contain any OVAL XML. They are intended for performing a manual review of the system.

4.2.2 Enabling/Disabling Content

To enable/disable a single Content stream:

1. **Left** click the check box to the left of the content stream name

To enable all Content streams:

1. **Right** click on any row
2. Click "Select All"

To disable all Content streams:

1. **Right** click on any row

2. Click "Clear All"

NOTE: *If multiple benchmarks are included in a SCAP 1.2 data stream, SCC splits each benchmark on the SCAP Content tab. This allows the end-user to enable/disable a specific benchmark within a larger data stream.*

4.2.3 Selecting a Profile

A profile is a collection of rules and is designed to allow the same set of SCAP content (XML) to perform different sets of checks based on end user need. SCAP content can contain one or more different profiles. By default, SCC enables the first profile found.

For USGCB, there is only one profile in the content, but for other content such as DISA, the end user will need to select the appropriate profile, according to the sensitivity of the computer being scanned. For DISA STIGS, below is the normal list of available profiles in each SCAP content stream.

- MAC 1 Public
- MAC 1 Sensitive
- MAC 1 Classified
- MAC 2 Public
- MAC 2 Sensitive
- MAC 2 Classified
- MAC 3 Public
- MAC 3 Sensitive
- MAC 3 Classified
- Disable Slow Rules
- CAT I Only

How many checks and results are impacted by changing the profile is completely dependent on the intent of the SCAP Content Author (not SCC). The checks in all profiles could be all the same, or they could differ greatly.

To select a profile:

1. **Left** click on the Stream name to populate the "Stream Details" window on the right
2. Select the desired profile from the Profile dropdown.

4.2.4 Selecting a Profile to use with All SCAP Content

To select a single profile, and apply it to all SCAP content:

1. **Right** click on the row to delete
2. Click "Set All Profiles"
3. A new form will open, showing a dropdown of all profiles found in all content.
4. Left click to select the desired profile
5. Click Save to save and close the form

4.2.5 Deleting Content

To delete a single content row

1. **Right** click on the row to delete

2. Click "Delete Selected Content"

To delete ALL Content

1. **Right** click on any row
2. Click "Delete All"

4.2.6 Viewing Stream Details

To view additional information about the SCAP Content:

1. **Left** click on the Stream Name
2. View the "Stream Details" form on the right pane.

A new form will appear with the Stream, Version, Status, Profile, OVAL Version, XCCDF Date, Patches Date, Title, Platform, Publisher, Description and Notice.

4.2.6.1 Saving SCAP Prose Reports

Once you have populated the Stream Details pane, a human readable 'prose' version of the XCCDF and OVAL files to either HTML or Text format may be produced. To use, a profile must be selected on the SCAP Content form. If no profile is selected, the buttons will be disabled.

The Prose report is a human readable representation of the SCAP content, very similar to the All Setting reports, but does not contain any scan data. It is meant to show the XCCDF rules and OVAL definitions in a logical tree structure format.

4.2.6.2 XCCDF Tailoring (SCAP 1.2)

This is a feature for advanced users wanting to modify how SCAP 1.2 benchmarks perform checks. Refer to the XCCDF Tailoring section 4.8 for details.

4.2.6.3 Deviations

This is a feature for advanced users wanting to justify why requirements cannot be met, and mark a settings as "Pass with Deviation". Refer to the Editing Deviations section 4.7 for details.

4.3 Performing a Scan

After installing and enabling the desired content and profile, the application is ready to perform compliance scanning.

1. Launch the SCC GUI
2. Select Scan Type
    - Local Scan
    - Single Remote Scan (Windows)
    - Multiple Remote Scan (Windows)
    - Cisco IOS Scan
3. Select Content Stream(s) and their respective applicable Profiles
4. Start Scan
5. View Reports

4.3.1 Select Scan Type

The SCC can review the local computer or remote computers over LAN/WAN connections. Select one of the following options:

4.3.1.1 Local Computer

This option instructs SCC to scan the computer in which the SCC software in installed.

4.3.1.2 Single Remote Computer (Windows)

This option instructs SCC to scan a single remote Windows computer over the LAN/WAN.

- Choose remote scan mode
    - Classic
        - Scan to be performed with remote API calls, no agent on remote computer
    - WMI
        - Scan to be performed by command line agent temporarily installed to target computer, and started and monitored via WMI
- A single NetBIOS computername or IP Address should be entered into the text field provided.

4.3.1.3 Multiple Remote Computers (Windows)

This option instructs SCC to scan a list of remote Windows computer over the LAN/WAN.

- Choose remote scan mode
    - Classic
        - Scan to be performed with remote API calls, no agent on remote computers
    - WMI

        - Scan to be performed by command line agent temporarily installed to target computers, and started and monitored via WMI
        - Scans are performed in parallel decreasing scan times for large numbers of computers.

- Create a new host file
    - Create a host list by querying Active Directory for the current domain
        - Options exist for validating this file
            - Validate host list using NSLookup to ensure computername is in DNS
            - Validate host list using NSLookup and Ping to ensure computername is in DNS and computer is online
- Choose an existing hosts file
    - This list should be in the form of a text file with a single computer listed per line.

4.3.1.4 Cisco IOS Config File

NOTE: As of this release, there is no official Cisco IOS content from DISA or NIST. Content can be developed by any end-user using the Cisco OVAL schema and ran via SCC. If Cisco IOS Content is made available, install into SCC, and refer to section 4.9 "Cisco IOS Config Scanning" for usage.

4.3.2 Select Content

Select content as described in section 4.2.

4.3.3 Performing Analysis

To perform a scan, click the '**Start Scan**' button.

To cancel a review, click the '**Cancel Scan**' button.

4.4 Editing Options

The SCC application has many end user customizable options, although the installation defaults are those most frequently used. After using SCC a few times, the end user may want to adjust some of these options, depending on their personal preferences.

1. Launch the SCC GUI
2. Click Options ->Show Options

4.4.1 Scan Options

4.4.1.1 Scan Methods

OPTION	DESCRIPTION
Perform SCAP Scan	This option enables SCAP scanning, and corresponds to the SCAP content tab. If this option is disabled, SCAP Streams that are enabled in the SCAP content tab will not be performed.
Perform OVAL Scan	This option enables standalone OVAL scanning, and corresponds to the OVAL content tab (which is only displayed if a user has installed standalone OVAL content). If this option is disabled, OVAL Streams that are enabled in the OVAL content tab will not be performed.
Perform OCIL Scan	This option enables standalone OCIL scanning, and corresponds to the OCIL content tab (which is only displayed if a user has installed standalone OCIL content). If this option is disabled, OCIL Streams that are enabled in the OCIL content tab will not be performed.

4.4.1.2 SCAP Processing

OPTION	DESCRIPTION
Run all content regardless of CPE-OVAL applicability	This option will ignore the content's CPE-OVAL results and continue processing the content against the system. This option can be used to run content that is not normally applicable to the target system (e.g. Red Hat SCAP content on a Debian system). Note that this option alters the standard SCAP rules for gathering certain objects which can result in incomplete results and/or false positives.
(SCAP 1.2 Only) Attempt to download external OVAL and XCCDF Tailoring files	This option allows the user to disable the SCAP 1.2 requirement of attempting to download OVAL and/or XCCDF Tailoring files from the internet, if specified in the content. If this option is enabled (default) and the SCAP 1.2 datastream lists a http reference for the OVAL or XCCDF Tailoring component, SCC will attempt to download it, and store it locally. Once it has been downloaded, it does not attempt again. This feature is not currently used by any production NIST or DISA SCAP content, but the feature is required for SCC to obtain SCAP 1.2

	validation.
Force OVAL results to 5.10.1 for SCAP 1.2 interoperability	SCC by default saves results in OVAL 5.11.1. However, this option could be enabled by the user for certain usage (primarily SCAP 1.2 validation) or tools that import OVAL results (but only support OVAL 5.10.1).

4.4.1.3 OVAL Processing

This set of options allows SCC to process currently available content in an efficient and accurate manner, however it does not comply with the letter of the law when it comes to the OVAL standard. Previous releases of SCC (1.0 - 3.0.x) ignored these OVAL directives, but they are now offered up as options, should end users want to comply completely with the OVAL standards.

Note: *Disabling any of these items could cause a dramatic slowdown in SCC's processing of SCAP content, and could cause certain SCAP content to return false positives.*

OPTION	DESCRIPTION
Ignore remote file systems during OVAL file scans (default is checked)	This option will ignore remote file systems, such as Windows shares, and UNIX NFS mount points. This option could be specified in the SCAP content as well, but in all of the publicly available SCAP content to date, the content authors have not specified to skip scanning of remote file systems. If this option is disabled, and the SCAP content does not specify to exclude remote file systems, SCC will scan all drives/mount points on the system, and will likely cause the application to slow down, dramatically in certain cases, and the results will potentially include issues from the server hosting the remote files. Until SCAP content is updated to ignore remote file systems, it is recommended to keep this option enabled in SCC.
Treat the OVAL 'equals' operation as 'case insensitive equals' (default is checked)	This option allows end users to override the instructions in the OVAL content and to ignore case of files and directories. Ideally this should be specified in the OVAL content, and enabling this option will cause warnings that results may not be as intended by the content author.
For the OVAL accesstoken_test, only collect security principles that have user rights (default is unchecked)	By default, the Windows accesstoken_test will collect user right information for all user accounts even if the accounts have no rights. Under certain circumstances (domain controllers), this could result in the collection of thousands of user accounts which may lead to extremely large result files and/or memory errors. If this option is enabled, then user right information will be collected only for user accounts that actually have user rights assigned.
Enable OVAL item creation threshold (default is checked; when this limit is	In certain circumstances, a combination of content issues, or system configuration can cause large numbers of OVAL items to be created. This causes two primary issues, the first being SCC's memory and CPU usage during the scan will increase, potentially to the point of crashing.

reached, items will be removed and results could be inaccurate)	Secondly, if SCC is able to complete the scan, the resulting XML files will be too large to create any Text or HTML reports from. This option caps the number of OVAL items created, on a per OVAL test basis, to the number specified in the form. This option can be updated by the user depending on their preference. If SCC runs out of memory and crashes even with this option enabled, it is recommended to lower the threshold by a sizable amount and re-run. If SCC reaches the threshold for a single test, the end result of the test will be 'error' as SCC will skip processing any additional items, and will not be able to make a final determination of compliance with regards to pass/fail, and the end user will likely need to perform the check manually to determine true compliance. This should not be a common occurrence, and the content author may need to be contacted, to determine if the test can be written in a method which does not create such a large volume of results. This option is enabled by default. By default, the OVAL Item Creation Threshold is set at 50,000.

4.4.2 Reporting Options

4.4.2.1 Select Reports

REPORT	DESCRIPTION
All Settings	This report contains detailed pass and fail results from each check performed. It is a large report and is not intended for printing
All Settings Summary	This report contains a summary of pass and fail results from each check performed.
Non-Compliance	Non-compliance reports contain detailed results from each failed check. It is a large report and is not intended for printing
Non-Compliance Summary	This report contains a summary of failed checks

4.4.2.2 Report File Types

FORMAT	DESCRIPTION
HTML	HTML formatted reports for viewing with a web browser
Text	Plain Text reports for viewing with a text editor such as Notepad or Wordpad.

4.4.2.3 XML Results

OPTION	DESCRIPTION
Save XCCDF Results	This option allows the user to disable saving the XCCDF XML files after the review. It should always be enabled unless drive space is limited. If this option is not enabled, multiple computer summary reports cannot

	be created.
Save OVAL Results w Full System Characteristics	This option allows the user to enable saving the OVAL XML files, which contain the detailed results from each review, and can be very helpful in debugging problems, or recreating reports after scans occur.
Save OVAL Results w/o Full System Characteristics	This option allows the user to save a slightly less verbose version of OVAL results, which exclude the System Characteristics, and is required by SCAP 1.2.
Save OVAL Results - Thin	This option allows the user to save even less data to OVAL results, which exclude the System Characteristics and Test results, and is required by SCAP 1.2.
Do Not Save OVAL Results	This option allows the user to not save OVAL XML results after each scan is complete.
Create ARF Results	This option creates the Department of Defense (DoD) Assessment Results Format (ARF) XML results based on ARF version 0.41.1
Validate XML Output Files	This option enables validating the XML results created by SCC.
Failed CPE OVAL Results	This option enables saving of Common Platform Enumeration (CPE) results for SCAP streams that are not applicable to the target system. This option should only be enabled for debugging why a SCAP stream is not performed against a target system. Enabling it will create numerous small XML files, which are not required for any other reporting purpose.

4.4.2.4 Summary Viewer

OPTION	DESCRIPTION
Save Summary Viewer	This option saves an HTML report that is created at the end of each scan, and provides an easy way to see all of the HTML/Text/XML results created by SCC during that scan session.
Summary Viewer Sorting	The summary viewer HTML report can be sorted by three fields. This report is primarily useful if more than one computer or content stream is used. Below is the default sort order and a description of each: 1. Session: The date/timestamp from when the scan started. 2. Stream : The SCAP content or OVAL datastream name being used 3. Host : The hostname for the target computer(s) being scanned. Note: The Summary Viewer can also be sorted manually by clicking on any column of the report after it's generated.

4.4.3 Logging Options

4.4.3.1 Logging Options

OPTION	DESCRIPTION
Save Screen Log	This option saves the analysis log printed to the "Status" screen to a text file for viewing after the review.

Save Debug Log	This option saves a large amount of additional information related to what occurred during a review. This option is disabled by default and should only be used when attempting to resolve errors in the application, as it will slow down the application and potentially use large amounts of disk space. Please refer to Appendix A.8 Debugging for additional information on SCC debug logs and their intended usage.
Suppress Warnings	This option will prevent warnings from being reported. As warnings are not critical, this option may be desired for certain users. This option may be useful in conjunction with 'ignore remote file systems' and 'ignore case' listed in the File Scanning section.

4.4.4 Output Options

4.4.4.1 Configuration Save Location

OPTION	DESCRIPTION
Save Configuration to the User's Home Directory	This option dynamically sets the base directory in which SCC saves it's configuration (5.0.1_options.xml) on a per-user basis. *Ex:* *C:\users\TestUser\SCC\Config\5.0.1_options.xml*
Save Configuration to the Running Application Directory	This option sets the based directory in which SCC saves it's configuration (options.xml) to the location SCC is running/installed. *Ex: C:\Program Files\SCAP Compliance Checker 5.0.1\options.xml*

4.4.4.2 Directory Options

OPTION	DESCRIPTION
Save Output to the User Home Directory	This option dynamically sets the base directory in which SCC saves all Logs and Results on a per-user basis. *Ex: C:\users\TestUser\SCC*
Save Output to the Running Application Directory	This option sets the based directory in which SCC saves all Logs and Results to the location SCC is running/installed. *Ex: C:\Program Files\SCAP Compliance Checker 5.0.1*
Save Output to a Custom Directory	This option allows the end user to specify any custom directory to save all SCC Results and Log. This can be a local path such as C:\SomeDirectory or a network share but only with the UNC path of \\ServerName\ShareName\SomeDirectory. Using a mapped drive such as Z:\SomeDirectory is known to cause errors and is not officially supported.

4.4.4.3 Subdirectory Options

OPTION	DESCRIPTION
Create 'Results' and 'Logs' Subdirectories	This option automatically creates subfolders of 'Results' and 'Logs' within the <user>\SCC directory
Create 'Date/Timestamp' Subdirectories	This option automatically creates a subfolder with the 'Date/Timestamp' within the results directory
Create 'SCAP', 'OVAL', 'OCIL' and 'ApplicationLog" directories	This option automatically creates a subfolder based on the content 'SCAP', 'OVAL', 'OCIL' within the results directory, and ApplicationLogs within the Logs directory
Create 'Content Name' Subdirectories	This option automatically creates a subfolder with the 'Content Name' within the results directory. This option is disabled by default.
Create 'Target Name' Subdirectories	This option automatically creates a subfolder with the 'Target Name' within the results directory. This option is disabled by default.
Create 'XML Subdirectory	This option automatically creates a subfolder with the 'Content Version' within the results directory

4.4.4.5 Permission Options

OPTION	DESCRIPTION
Allow SCC to set restricted permissions on SCC created Logs and Results	This option allows SCC to set restricted permissions on the Logs and Results (XML, Text, HTML) created by SCC. This can be useful especially if results are set to write back to the application install, or some other location were non-privileged users have read access. On Windows: SCC sets the permissions to be the user running SCC, Administrators, and System Disabling this option defaults back to the OS defaults.

4.4.4.1 Configuration Save Location

OPTION	DESCRIPTION
Save Configuration to the User's Home Directory	This option dynamically sets the base directory in which SCC saves it's configuration (5.0.1_options.xml) on a per-user basis. *Ex:* *C:\users\TestUser\SCC\Config\5.0.1_options.xml*
Save Configuration to the Running Application Directory	This option sets the based directory in which SCC saves it's configuration (options.xml) to the location SCC is running/installed. *Ex: C:\Program Files\SCAP Compliance Checker 5.0.1\options.xml*

4.4.5 XML Validation Options

4.4.5.1 XML Schema Validation

OPTION	DESCRIPTION
Perform XML Schema Validation on Input Files	This option validates that the XML content is syntax error free before performing the review.
Perform XML Schema Validation on Output Files	This options validates that the XML result files are syntax and error free after creation.
Cancel Scan(s) on XML Digital Signature Validation Failure	This option will automatically cancel a scan if the signed XML file(s) fail XML digital signature validation.

4.4.5.2 XML Digital Signatures

OPTION	DESCRIPTION
Perform XML Digital Signature Validation	This option will validate signed XML content files prior to execution.
Cancel Scan(s) on XML Digital Signature Validation Failure	This option will automatically cancel a scan if the signed XML file(s) fail XML digital signature validation.

4.4.6 SSH Options

SCC has the ability to copy results after each scan via SSH to a centralized server for easier data collection. This feature is disabled by default. To enable:

1. Launch the Graphical User Interface of SCC
2. Click Options ->Show Options -> SSH Options
3. Enable SSH Report Transfer
4. Select Reports to Transfer
5. Enter Hostname or IP Address
6. Enter credentials
7. Enter remote SSH directory
8. Click Test Connection
9. Click Save

Note: *SSHv2 is supported, SSHv1 is not.*

4.4.6.1 SSH Server Information

OPTION	DESCRIPTION
SSH Server Hostname/IP Address	Enter the DNS hostname or IP Address of the SSH server to copy result to
SSH Server Port	Enter the port which the SSH server is listening (normally 22)
Transfer Results to Remote SSH Directory	By default, this is set as the user's home directory (e.g. /home/<ssh username>) but can be changed here to reflect the desired directory you would like the reports to be transferred to.

4.4.6.2 SSH User Login Information

OPTION	DESCRIPTION
Connect to SSH Server with Username/Password	Select this option if you plan to authenticate with username/password combination
Connect to SSH Server with Private Key/Passphrase	Select this option if you plan to authenticate with a private key. ***Note:*** *SCC only supports private keys that are secured with a private key passphrase*
SSH Username	Required for either Username/Password or Private key authentication
User Password	Only required if Username/Password authentication has been selected
User Private Key	Only required if Private Key/Passphrase authentication has been selected
Private Key Passphrase	Only required if Private Key/Passphrase authentication has been selected

4.4.6.3 Reports to Transfer

OPTION	DESCRIPTION
Transfer XML Results to SSH Server	Transfers only the XML result files generated by SCC
Transfer HTML Reports to SSH Server	Transfers the HTML reports generated by SCC
Transfer Text Reports to SSH Server	Transfers the Text reports generated by SCC
Transfer Error Logs to SSH Server	Transfers any generated Error Logs to the SSH server
Transfer Debug Logs to SSH Server	Transfers any generated Debug Logs to the SSH server

4.4.6.4 Transfer Options

OPTION	DESCRIPTION
Delete Local Results After Transfer	This option will delete the local results off of the machine after SCC has successfully transferred the files to the SSH server

4.5 Viewing Reports

4.5.1 Viewing Single Computer Reports

After the SCC software completes the review, the reports can be viewed by clicking:

Results -> Open Results Directory

or

Results -> Recent Reports

The Data Directory, which contains both the results and logs, is configurable based on user preferences. Refer to "Editing Options" section of this manual for details. By default, the data is stored in a subdirectory called "SCC" in the user's home directory, but can be configured to store results to the installation directory, or any custom directory.

4.5.2 Viewing Recent Reports from the GUI

The feature of *"Results -> Recent Reports*" allows the user to quickly view recently created reports without having to browse through the directory structure.

To increase the number of recent reports listed, refer to the "Editing Options" section of this manual.

4.6 SCAP scanning with OCIL

This section is only applicable to SCAP content which contain OCIL (Open Checklist Interactive Language) Qustionaires. Currently the NIST USGCB Content for Windows 7 is the only content with OCIL.

The order of operations for a SCAP 1.1/1.2 data stream with OCIL is as follows:

1. User enables SCAP 1.1 or 1.2 content which contains OCIL Questionaires
2. User clicks "Analyze Computers"
3. A form called "SCAP/OCIL Stream Documents" opens displaying SCAP streams which contain OCIL checklists.
4. User answers questionnaires for the target computer(s)
5. After questionnaires have been completed, the OVAL scanning proceeds
6. OVAL and OCIL results are collected into the XCCDF results
7. HTML/Text reports are created which contain both the OVAL and OCIL results

4.6.1 Selecting OCIL questionaires on the SCAP/OCIL Stream Documents form

This form contains a list of SCAP streams which were selected on the Edit -> Content and Options -> SCAP Content tab, which contain an OCIL checklist.

- To answer questions for the OCIL questionnaire that are enabled, click "Start OCIL Review".
- To skip answering OCIL questionnaire and proceed with automated scanning, press "Continue Analysis". This will cause SCC to list all of the questions as "Not Checked".
- To resume from a previous partially completed OCIL questionaire, **right** click on the OCIL document, and click "Resume Previous", then select the desired file to resume from.

4.6.2 Answering Questions on the OCIL Document Form

This form allows you to answer any questions in the OCIL questionnaire. All of the question titles will be listed in the tree on the left hand side. To answer a question, click at the leaf node, which has a grey circle. This will populate the associated question on the right hand side.

4.6.2.1 Entering Comments

For each question, the user can manually enter a comment which may help explain the results. To enter a comment, type in the comment field and click "Save Comment".

4.6.2.2 Entering Content Mandated Artifacts

The OCIL content can also ask specifically for artifacts, which will cause a new form to appear, which contains:

FIELD	DESCRIPTION
Title	Content provided title

Description	Content provided description, likely explaining what data the end user should provide
Data	Location for the end user to enter data as specified in the Description field.
Save	After entering Data, click Save to close this form.

4.6.2.2 Save and Close

When you have completed all of the questions, click "Save & Close". This will take you back to the OCIL Questionnaire Form, or to the next Questionnaire if more than one has been enabled.

4.6.3 Proceeding to the automated OVAL checks

If you have answered all of the OCIL Questionnaire, click "Continue Analysis" to proceed to the automated OVAL tests.

4.7 Editing Deviations

Deviations will change the status of deviated checks from Fail, Error or Unknown to Pass and will update the computer's compliance score. Only enter deviations that have been approved for your organization.

Deviations are only applied at review time, and only if a check fails, they do not disable a check or prevent it from being performed. To edit user specified deviations:

1. Launch the Graphical User Interface of SCC
2. Edit -> Content and Options -> Deviations Tab

4.7.1 Enabling Deviations

To enable the use of Deviations, click the check box next to "Enable Deviations." This does not mean that deviations are currently defined, just that the functionality has been enabled or disabled.

4.7.2 Select a SCAP Stream

Select the desired SCAP Stream from the drop down on the upper left of the form. The list will be in the format of <scap stream>-<version>. Examples:

USGCB-xpfirewall-v2.0.0.0

USGCB-winxp-v2.0.0.0

4.7.3 Select a Stream Profile

If more than one than one Profile is available in the selected SCAP Stream, select the Profile from the drop down on the upper right corner of the form. The first available profile will automatically be populated into the drop down.

4.7.4 Select a Check

To edit a deviation, click on the desired row containing the CCE reference or check tile in the white list box in the center of the form. This will populate the fields on the bottom half of the form.

4.7.5 Activating Deviations

Activating deviations requires obtaining a specific unlock code from a separate application called the SCC Unlocker, which provides the unlock codes for all SCAP content. This application is separate from the SCC and must be obtained directly from SPAWAR. This application is designed to be available only to person(s) in your organization that can officially approve deviations.

In order for deviations to be used to change the pass/fail status of checks, the "Authority" field must contain the person who authorized the deviation and the "Unlock Code" field must contain the correct code from SCC Unlocker application. Additionally, the "Remark" field should be

used to explain why the deviation is necessary. Justification for any deviations is included in the application reports.

After the "Authority" field is populated with any text and the correct code is entered into the "Unlock Code" field, the check box next to "Deviation is Active" will be selected, and the text in the Deviation box will change from grey to blue.

Note: *Unlock Codes are unique per check performed. In other words, an Unlock Code for Check1 will not work for Check2.*

Note: *Unlock Codes are unique per each version of SCAP content. In other words, an Unlock Code for Check1 of content version 1.2.0.0 will not be valid for Check1 of content version 1.3.0.0, as the requirements for this check may have changed with revised version.*

4.8 XCCDF Tailoring

SCAP 1.2 specifications allow for a separate 'tailoring' XML file which allows users to customize certain portions of the XCCDF stream, without modifying the source XML file. Customizations include:

- Creation of a new profile
  - All modifications will be reported under a new profile, with the original profile name followed by "_tailored'
- Selecting and deselecting rules and groups
  - This allows users to disable rules that may cause incorrect results, or take too long to complete.
  - Results will be marked as 'not selected'
- Modifying refine-rules, values and refine-values
  - This allows users to modify certain rules to meet their organizational requirements. Note that not all rules will have modifiable values, and OVAL XML content may need to be edited.

SCC supports this feature, and provides a graphical interface for creating and editing the XCCDF tailoring file.

4.8.1 Select SCAP 1.2 Stream to Tailor

Field	Description
Stream	Select a SCAP 1.2 stream from the dropdown list, or click install to add new to the content collection.
Tailoring File	This field will be auto-popluated by SCC when users click "Save".
Profile(s)	Select the profile to tailor. This will be updated to the 'tailored' profile after clicking 'Save'.

4.8.2 Selecting/Deselecting Groups and Rules

To enable/disable rules or groups:

1. Left click on the checkbox on the far left on any row listed with a Type of "Group" or "Rule".
2. Enabling or Disabling a group will cascade Enable/Disable to all sub-groups and rules.
3. Enabling/Disabling can also be perform by left clicking on the row, and clicking the check-box in the right hand window.

Note: Per XCCDF 1.2 specifications, if a Group is disabled, no sub-groups or rules under it are evaluated (even if they are enabled manually). If a group is enabled, the sub-groups and rules are processed based on their individual selected/deselected status.

4.8.3 Refine Rules

To refine a rule:

1. Left click on a row listed with a Type of "Refine-Rule"
2. Edit any of the available fields in the right hand window
   a. Weight
   b. Role
   c. Severity
   d. Selector
   e. Remarks

Note: This feature has not been seen in any publicly available content, so end users may not see "Refine-Rules" in any rows.

4.8.4 Values and Refine-Values

To modify a value:

1. Click on any row in tree listed with a Type of "Value"
   A. Enter the desired value in the 'Set Value To' field, and click "Apply Value"
   OR
   B. Select the Refined Value Selector

   Note that the Refine Value Selector may only have a single row, unless the SCAP content contains multiple options to choose from.

Note: Values and refine-values may not be present in content. As of release of SCC 5.0, NIST USGCB content had values and refine values, but DISA STIG content did not.

4.8.5 Saving XCCDF Tailoring

Click Save and Close. The selected profile on the main SCC form should be updated to reflect the new <Profile>_tailored profile.

4.8.6 Entering XCCDF Tailoring File Creator Info

After clicking Save, a form will appear with the following fields. These will all be saved to the resulting XML results and HTML/Text reports if enabled.

Field	Description
Agency/Organization	Enter your Agency/Organization Name
Full Name	Enter your full name
Notes	Enter any notes that help explain why this XCCDF Tailoring file was created.
Version	Enter a version for this XCCDF Tailoring file
Status	Select the status of this XCCDF Tailoring file (Draft, Accepted, Deprecated, Incomplete, Interim)

4.9 Cisco IOS Config Scanning

This option instructs SCC to scan an existing Cisco IOS configuration file. The file format required for this type of assessment is very specific. To create a configuration file suitable for using in SCC:

1. Logon to the device with full (level 15) privileges (enable mode)
2. Type “show tech" saved to a single text file
3. Save the file as “<devicename>_<date>.txt”

   NOTE: Save this file as Text Only with Line Breaks using a plain text editor such as Notepad. Do not use Microsoft Word or other document editor. Only one device per file
4. Disable any Windows or UNIX SCAP/OVAL content, otherwise many content errors will be reported
5. Enable just Cisco IOS specific SCAP/OVAL content

4.9.2 Browse for Cisco IOS Config File

This option allows the end user to select a single file, either a text file (.txt) containing single Cisco IOS configuration file, or a zip file containing a collection of Cisco IOS configuration files.

4.9.3 Browse for a directory containing Cisco IOS config files

This option allows the user to select a directory which contains a collection of text (.txt) based Cisco IOS configuration files.

4.9.4 Unsupported Show Command Remediation

In the event that one or more IOS line tests abort due to unsupported "show" commands, take note of the list of unsupported commands that are listed at the end of the analysis. Most Cisco IOS content is likely to attempt collection of "show" command output that is not provided by the "show tech" or "show tech-support" commands by default. The best recourse is to manually execute any unsupported commands and append their output to the "show tech" command output:

1. Logon to the device with full (level 15) privileges (enable mode)
2. Execute the listed commands
3. Copy the output of each command and append it to the original "show tech" output file with a leading header on its own line that specifies the command that generated the output
4. Ensure each header consists of a sequence of 18 hyphens, a space, a show command, another space, and 18 more hyphens for consistency with the default "show tech" command output

4.10 Standalone OVAL Usage

Standalone OVAL content usage is designed primarily for advanced SCC users, such as content authors who wish to run OVAL content without creating an entire SCAP benchmark. It can also be used to perform vulnerability scanning using existing OVAL vulnerability content. No standalone OVAL content is currently bundled with SCC.

1. Launch the Graphical User Interface of SCC
2. Follow instructions for Installing & Configuring Content (Section 4.2)
3. If standalone OVAL content is found during the content install, an OVAL content tab will appear for enabling/disabling content.

SCC will also search the <SCC Install>\Resources\OVAL_Content directory and subdirectories for OVAL XML files.

Note: *OVAL content that is part of a SCAP Stream, such as USGCB, or DISA STIGS should be installed into the SCAP Content, not in the OVAL content. OVAL content included in a SCAP Stream is designed to work with XCCDF and CPE. SCC might be able to process the OVAL file as 'raw OVAL' but unexpected errors may exist.*

4.11 Standalone OCIL Usage

Standalone OCIL (Open Checklist Interactive Language) content usage is designed primarily for advanced SCC users, such as content authors who wish to run OCIL content without creating an entire SCAP benchmark. No OCIL content is currently bundled with SCC.

4.11.1 Installing OCIL content

1. Launch the Graphical User Interface of SCC
2. Follow instructions for Installing & Configuring Content (Section 4.2)
3. If standalone OCIL content is found during the content install, an OCIL content tab will appear for enabling/disabling content.

SCC will also search the <SCC Install>\Resources\OCIL_Content directory and subdirectories for OCIL XML files.

Note: *OCIL content that is part of a SCAP Stream, such as DISA STIGS, should be installed into the SCAP Content, not in the OCIL content. OCIL content included in a SCAP Stream is designed to work with XCCDF, OVAL and CPE. SCC might be able to process the OCIL file as 'raw OCIL' but unexpected errors may occur. For more information please see section 4.4.*

OCIL schema validation occurs during installation of the OCIL content. If the OCIL content is deemed invalid, SCC will inform the user via a dialog box but will continue the installation process. The user will be notified of the result of the installation process in a separate dialog box.

4.11.2 Performing a standalone OCIL analysis

4.11.2.1 Selecting OCIL Documents

This form contains a list of SCAP streams which were selected on the Edit -> Content and Options -> SCAP Content tab, which contain an OCIL checklist.

- To answer questions for the OCIL questionnaire that are enabled, click "Start OCIL Review".
- To skip answering OCIL questionnaire and proceed with automated scanning, press "Continue Analysis". This will cause SCC to list all of the questions which have not been answered as "Not Checked".
- To resume from a previous partially completed OCIL questionaire, **right** click on the OCIL document, and click "Resume Previous", then select the desired file to resume from.

4.11.2.2 Creating and Selecting OCIL Targets

Unlike the automated portions of SCC, which the target is always a computer, whose hostname is automatically populated by programmatic means during the scan, with OCIL, the target could be a computer/system or a user/person, and each will need to be manually entered.

To create a new system target, click on the 'add a new system target' in the in upper left corner of the form. Then enter in as much information as you have.

FIELD	DESCRIPTION
System Name	The name of the system, generally a computer, which is the target for the checklist. This field is mandatory.
IP Address	Optional field to report on the IP Address associated with this system.
Organization	Optional field to document the organization that the system is a part of.
Description	Optional field to enter any other information about this system that might be relevant.

To create a new user target, click on the 'add a new user target' in the in upper left corner of the form. Then enter in as much information as you have.

FIELD	DESCRIPTION
Full Name	The name of full name of the person being interviewed. This field is mandatory.
Email	Optional field to report on the email address of the person being interviewed.
Organization	Optional field to document the organization that the person is a part of.
Description	Optional field to enter any other information about this person that might be relevant.

After creating and selecting the desired targets, click "Continue".

4.11.2.3 Answering Questions on the OCIL Document Form

This form allows you to answer any questions in the OCIL questionnaire. All of the question titles will be listed in the tree on the left hand side. To answer a question, click at the leaf node, which has a grey circle. This will populate the associated question on the right hand side.

4.11.2.3 Entering Comments

For each question, the user can manually enter a comment which may help explain the results. To enter a comment, type in the comment field and click "Save Comment".

4.11.2.4 Entering Content Mandated Artifacts

The OCIL content can also ask specifically for artifacts, which will cause a new form to appear, which contains:

FIELD	DESCRIPTION
Title	Content provided title
Description	Content provided description, likely explaining what data the end user should provide
Data	Location for the end user to enter data as specified in the Description field.
Save	After entering Data, click Save to close this form.

4.4.2.2 Save and Close

When you have completed all of the questions, click "Save & Close". This will take you back to the OCIL Questionnaire Form, or to the next Questionnaire if more than one has been enabled.

4.11.3 Generating Reports

If you have answered all of the OCIL Questionnaire, click "Create Reports" to proceed to creating reports with the results.

4.12 Post Scanning Report Generation

SCC, by default, creates most of the commonly used reports during each scan. However, additional reports can be from previous scan results. These are completely optional depending on your desired usage.

4.12.1 Select Directories

OPTION	DESCRIPTION
Source Directory	Location for the application to scan for XCCDF and/or OVAL XML results from previous reviews. This option is recursive (all subfolders will be scanned for files to use).
Destination Directory	Location where summary reports are to be saved.
Open Destination Directory when processing is complete	This opens Windows Explorer to the directory containing the new summary reports, when the processing is complete.

4.12.2 Reports

4.12.2.1 Generate Summary SCAP Reports (from XCCDF results)

SCC can generate multi-computer summary reports from the XCCDF XML (SCAP) results created by the SCC or other SCAP Validated applications.
To generate summary reports from existing XCCDF XML files:

Note: To create reports based on a subset of computers in the organization, organize the consolidated data in a directory structure similar to the example listed below:

/Entire Organization
/ Sub Organization 1
/ Sub-Sub Organization
/ Sub Organization 2
/ etc..

If the SCC is pointed at the entire organization, or any subset, the summary reports will only contain the desired subset of computers.

4.12.2.1.1 Select Reports to Generate

OPTION	DESCRIPTION
Site Summary	This report provides a consolidated list of checks, with a single CCE reference and the Pass, Fail, Error, Unknown, Not Applicable, Not Checked, and Not Selected occurrences for each check.
Site Summary Non-Compliance	This report provides a consolidated list of checks, with a single CCE reference and the Fail, Error and Unknown occurrences for each check that had a fail or an error status.

Computer List	This report lists the latest results for all computers reviewed and the Review Time, Pass, Fail, Error, Unknown, Not Applicable, Not Checked, Not Selected, Total along with the Original and Adjusted Scores.
Computer List Historical	This report lists all results for all computers reviewed, and the Review Time, Pass, Fail, Error, Unknown, Not Applicable, Not Checked, Not Selected, Total along with the Original and Adjusted Scores.

4.12.2.2 Generate Detailed SCAP Reports (from ARF or XCCDF/OVAL results)

SCC can regenerate single computer detailed reports from the XCCDF XML and OVAL XML (SCAP) results created by the SCC or other SCAP Validated applications.

4.12.2.2.1 Select Reports to Generate

REPORT	DESCRIPTION
All Settings	This report contains detailed pass and fail results from each check performed. It is a large report and is not intended for printing.
All Settings Summary	This report contains a summary of pass and fail results from each check.
Non-Compliance	Non-compliance reports contain detailed results from each failed check. It is a large report and is not intended for printing.
Non-Compliance Summary	This report contains a summary of the failed checks.

4.12.2.3 Generate Detailed OVAL Reports (from standalone OVAL results)

SCC can regenerate single computer detailed reports from the standalone OVAL XML results created by the SCC or other SCAP Validated applications.

4.12.2.3.1 Select Reports to Generate

REPORT	DESCRIPTION
All Settings	This report contains detailed pass and fail results from each check performed. It is a large report and is not intended for printing.
All Settings Summary	This report contains a summary of pass and fail results from each check.
Non-Compliance	Non-compliance reports contain detailed results from each failed check. It is a large report and is not intended for printing.
Non-Compliance Summary	This report contains a summary of the failed checks.

4.12.3 Select File Format(s) of Generated Reports

FORMAT	DESCRIPTION
HTML	HTML formatted reports for viewing with a web browser

Excel	Excel Spreadsheet versions with separate tabs per SCAP stream

4.12.4 Generate Reports

To create the summary reports, click Generate. The status window will display the progress.

Note: *Summary reports can also be created with a command line parameter, based on the settings configured in the GUI. Please refer to the Using the Software via Command Line for additional information.*

4.12.5 Viewing Reports

After Multi-Computer Summary Reports are created a Windows Explorer window may open (based on user preferences), and the reports specified to be created will be available in HTML and/or Excel spreadsheets. To view, double click on any of the files.

5. COMMAND LINE USAGE

SCC has a separate executable for command line usage which is included in the installation package as 'cscc.exe'. The Command-line SCAP Compliance Checker (CSCC) allows for scripted or automated reviews by other applications or scheduled tasks.

Any changes made via the SCC GUI such as content installation, or application preferences impact the command line interface and vice versa, as the options for both interfaces are saved to the same 'options.xml' file located in the SCC installation directory.

Note: *All command line usage requires Administrator privileges.*

5.1 Basic Command Line Usage

Below is a quick overview of how CSCC works.

1. Open a Command Prompt with an account that has Administrator privileges.
2. Install any additional SCAP Content into CSCC.
3. Run the Configuration Menu option of CSCC (--config).
4. View available SCAP content included with CSCC.
5. Enable SCAP Content and Select the desired profile from each SCAP Content stream.
6. Scan Computer(s) with Enabled SCAP Content.
7. View reports.

To view all available command line options, use the -? parameter.

```
cscc.exe -? or cscc.exe --help
```

5.1.1 Open a Command Prompt

Open an Admin command prompt and change directory to the SCC installation directory.

Example:

Start -> Run -> cmd

```
c:
cd "\Program Files\SCAP Compliance Checker 5.0.1"
```

5.2 Command Line Configuration Parameters

5.2.1 Installing Content into SCC

Below are the parameters for installing content and configuring application options. All of the following options must be used individually, and are not compatible with any other parameter. These parameters are designed to be performed before scanning occurs.

--config

Opens a command line menu which displays several configuration options.

Note: *See section 5.2.2 for more information on the command line configuration menu.*

--cisco <path>

Conduct an offline review against a Cisco IOS configuration file or ZIP archive of multiple configuration files located at the given file path.

```
Example:  cscc.exe --cisco <path>
```

--setProfileAll <profile>

Set a profile to be applied to all content installed in SCC, if applicable. If a profile cannot be applied to a content stream it is not applicable.

```
Example cscc.exe --setProfileAll MAC-3_Sensitive
```

--setProfile <profile> <benchmark id>

Set a profile to be applied to a specified content stream.

```
Example cscc.exe --setProfile MAC-3_Sensitive Windows_10_STIG
```

-da

Disable all SCAP and OVAL content

-ea

Enable all SCAP and OVAL content

-ua

Uninstall all SCAP and OVAL content

-is <path>

Install SCAP (1.0, 1.1, 1.2) content stream from a zip file, or from a single SCAP 1.2 datastream XML file. This will enable it by default, and set the first profile found as active.

```
Example:  cscc.exe -is <path>
Example:  cscc.exe -is --force <path>
```

-iv <path>

Install OVAL content or optional External Variables Files from a single xml file or a zip file containing multiple xml files.

```
Example:   cscc.exe -iv <path>
Example:   cscc.exe -iv --force <path>
```

-setOpt <OptionName> <ValueToSet>

Advanced user setting which allows command line configuration of any SCC setting. Can be called several times via one command line call to cscc.

```
Example1: cscc.exe --setOpt dirTimestampEnabled 0

Example2: cscc.exe --setOpt dirTimestampEnabled 0 --setOpt
debugEnabled 1
```

To set a value to an empty string, enter the value as all caps NULL

Available options can be found in section *5.3: Option Descriptions and Datatypes*

--getOpt <OptionName>

Advanced user setting which queries any SCC setting.

```
Example1: cscc.exe --setOpt dirTimestampEnabled
```

--listAllProfiles

List all profiles according to the installed content. Note that not all profiles are available to all content streams.

```
Example1: cscc.exe --listAllProfiles
```

--listAllBenchmarks

List all benchmarks according to the content installed on the system. Useful when setting a profile for specific content.

```
Example1: cscc.exe --listAllBenchmarks
```

Available options can be found in section *5.3: Option Descriptions and Datatypes*

5.2.2 Editing Options for Command Line Use

Many of the options for SCC can be edited via the --config command line parameter of CSCC. Any changes made with the --config menu will be saved to the 'options.xml' file which is located in the installation directory of SCC.

For more in-depth descriptions of each option available for configuration, please refer to section 4.4, "Editing Options".

```
cscc.exe --config

   SCC 5.0.1 configuration edit menu.
```

```
Make menu selection:

1. Configure SCAP content
2. Configure SCAP profiles
3. Delete SCAP content
4. Configure OVAL content
5. Delete OVAL content
6. Configure Options
7. Exit and save changes
8. Exit without saving changes
9. Exit, save changes, and execute scan

SCAP Processing is Enabled

- 4 of 25 SCAP streams are enabled
OVAL Processing is Disabled

- 0 of 0 OVAL streams are enabled
Enter menu selection:
```

1. Configure SCAP content

```
Press ENTER view more streams OR:
Enter content number to enable or disable content.
Other command options are: 'all', 'clear', or you can enter
a range N-N
Type 'back' or '0' to return to the previous menu
```

2. Configure SCAP profiles

```
Press ENTER view more streams OR:
Enter content number to view available profiles (type
'back' or '0' to return)
Enter profile number to set selected profile (type 'back'
or '0' to return):
```

3. Delete SCAP content

```
Press ENTER view more streams OR:
Enter content number to delete content.
('all' is allowed, type 'back' or '0' to return):
```

4. Configure OVAL content

5. Delete OVAL Content

6. Configure options

SCC 5.0.1 Options menu.

```
 1. Scanning Options
 2. Reporting Options
 3. Logging Options
 4. Output Options
 5. XML Validation Options
 6. SSH Options
 7. SCAP 1.2 XCCDF Tailoring
 8. Delete SCAP 1.2 XCCDF Tailoring File
Enter menu selection (type 'back' or '0' to return):
```

SCC 5.0.1 SCAP/OVAL OPTIONS MENU

```
     -- Content Scan Methods
         1. [X] Perform SCAP Scan
         2. [ ] Perform OVAL Scan
     -- SCAP Processing
         3. [ ] Run all content regardless of CPE-OVAL
     applicability
         4. [X] Attempt to download external OVAL and
     XCCDF Tailoring files.
         5. [ ] Force OVAL results to 5.10.1 for SCAP 1.2
     interoperability.)
     -- OVAL Processing
         6. [X] Ignore remote file systems during OVAL
     file scans
         7. [ ] Treat the OVAL 'equals' operation as 'case
     insensitive equals'
         8. [X] Enable OVAL item creation threshold
         9.     Item creation threshold: 50000
        10. [ ] Process the OVAL accesstoken_test by user
     right
     Enter menu selection (type 'back' or '0' to return):
```

SCC 5.0.1 REPORTING OPTIONS MENU

```
-- Select Reports
    1. [X] Generate 'All Settings' report
    2. [ ] Generate 'All Settings Summary' report
    3. [X] Generate 'Non-Compliance' report
    4. [ ] Generate 'Non-Compliance Summary' report
-- Report File Types
    5. [X] Generate reports as HTML
    6. [ ] Generate reports as Text
-- XML Results
```

```
    7. [X] Save generated XCCDF XML files
    8. [X] Save generated OVAL XML files - Full w/ System
Characteristics (Default)
    9. [ ] Save generated OVAL XML files - Full w/o System
Characteristics
   10. [ ] Save generated OVAL XML files - Thin
   11. [X] Save generated OCIL XML files
   12. [X] Save generated NIST ARF XML files
   13. [ ] Save failed CPE XML results files
-- Summary Viewer
   14. [X] Save Summary Viewer HTML report
   15. Summary Viewer Sort Level 1: [Session]
   16. Summary Viewer Sort Level 2: [Stream]
   17. Summary Viewer Sort Level 3: [Host]
Enter menu selection (type 'back' or '0' to return):
```

SCC 5.0.1 LOGGING OPTIONS MENU

```
-- Logging and Debugging
    1. [ ] Save screen logs
    2. [ ] Save debug logs
    3. [ ] Suppress warnings
Enter menu selection (type 'back' or '0' to return):
```

SCC 5.0.1 FILE/DIRECTORY OPTIONS MENU

```
     -- Configuration Save Location
         1. [ ] Save Configuration to the User's Home
     Directory
         2. [X] Save Configuration to the Running
     Application Directory
     -- Output Directory
         3. C:\Users\<username>\SCC
     -- Output Subdirectory Options
         4. [X] Create 'Results' and 'Logs' subdirectories
         5. [X] Create 'Date/Timestamp' subdirectories
         6. [X] Create 'Content Type
     (SCAP/OVAL/OCIL/ApplicationLogs)' subdirectories
         7. [ ] Create 'Target Name' subdirectories
         8. [ ] Create 'Content Name' subdirectories
         9. [X] Create 'XML' subdirectories
     -- Output Filename Options
```

```
   10. [X] Use 'Target Name' in report filenames
   11. [X] Use 'SCC Version' in report filenames
   12. [X] Use 'Date/Timestamp' in report filenames
Enter menu selection (type 'back' or '0' to return):
```

SCC 5.0.1 XML VALIDATION OPTIONS MENU

```
-- XML Schema Validation
   1. [ ] Perform XML Schema Validation on Input
Files
   2. [ ] Perform XML Schema Validation on Output
Files
   3. [ ] Perform XML Schema Validation on Input
Files during installation
-- XML Digital Signatures
   4. [ ] Perform XML Digital Signature Validation
   5. [ ] Cancel Scan(s) on XML Digital Signature
Validation Failure
Enter menu selection (type 'back' or '0' to return):
```

SCC 5.0.1 SSH Options menu.

```
*Note: only SSHv2 is supported
-- File Transfer Options
   1. [ ] Enable file transfers
   2. [ ] Delete local reports after transfer
-- Reports to Transfer
   3. [X] XML
   4. [X] HTML
   5. [ ] Text
   6. [X] Error Logs
   7. [ ] Debug Logs
-- Server Information
   8. Hostname/IP Address:
   9. Port: 22
-- Select Username/Password connection, or Private
Key connection
   10. [X] Connect using Username/Password
   11. [ ] Connect using Private Key and Passphrase
-- Directory Information
   12. Local results directory:
   13. Remote SSH directory:
-- Test SSH Connection
```

```
   14. Test SSH connection to:
Enter menu selection (type 'back' or '0' to return):
```

Select SCAP Content to install, enable, or disable XCCDF Tailoring

```
1.  [ ] USGCB-Windows-7-2.0.5.1.zip
Enter content number to configure tailoring
(type 'back' for previous menu or '0' to return to
main menu):
```

Select XCCDF Tailoring file to delete

```
No SCAP 1.2 Content XCCDF Tailoring files to delete.
 (Type '0' or 'back' to return to main menu):
```

7. Exit and save changes

8. Exit without saving changes

9. Exit, save, and execute scan

5.4 Option Descriptions and Datatypes

Below are all of the options that can be configured via the --setOpt command line parameter, which is primarily designed for advanced users to automate command line reviews.

OPTION	DESCRIPTION	DATATYPE
GENERAL SCANNING OPTIONS		
scapscan	Enable standalone SCAP Scanning	Boolean (0/1)
ovalscan	Enable standalone OVAL Scanning	Boolean (0/1)
ocilscan	Enable raw/standalone OCIL Scanning (GUI Only)	Boolean (0/1)
reviewType	Type of review	String ('local', 'cisco', 'remote', 'multiremote' (remote/multiremote for Windows only))
offlineConfigPath	Target if 'reviewType' equals 'cisco', This is a fully qualified path to a valid CiscoIOS configuration text file	String
REMOTE SCANNING OPTIONS (WINDOWS ONLY)		
hostName	Target of SCC scan if 'reviewType' equals 'remote'	String
hostFile	Fully qualified path to a text file containing NetBIOS names of Windows computers, one per line	String
remoteWMIEnabled	WMI Remote is enabled, used to determine if remote Windows scans should be WMI based	Boolean (0/1)
remoteRefreshDelay	WMI Remote Refresh Delay, Number of seconds between WMI status updates	Integer
remoteMaxThreads	Maximum number of WMI scanning threads to create on 64 bit Windows	Integer
remoteMaxThreads32	Maximum number of WMI scanning threads to create on 32 bit Windows	Integer
SCAP PROCESSING OPTIONS		
ignoreCPEOVALResults	Run SCAP content even if CPE OVAL applicability fails	Boolean (0/1)
downloadExternalFiles	Download external SCAP 1.2 content files	Boolean (0/1)
forceOVAL510	Force OVAL results to be compliant with 5.10.1 for SCAP 1.2 validation purposes	Boolean (0/1)
OVAL PROCESSING OPTIONS		

ignoreRemoteFileSystems	Do not perform any file searches on remote file systems	Boolean (0/1)
ignoreCase	Ignore case specific content requirements for searching files, paths, registry keys, etc	Boolean (0/1)
itemCreationThresholdEnabled	Enable setting a maximum number of items to create, to save memory usage in SCC	Boolean (0/1)
itemCreationThreshold	Numeric value for item creation threshold if itemCreationThresholdEnabled equals 1	Integer
OVAL PROCESSING OPTIONS (UNIX ONLY)		
maskPasswords	Do not display UNIX password hashes to reports or XML files, does not impact test accuracy.	Boolean (0/1)
useGetpwent	Use the system command of getpwent instead of parsing /etc/passwd	Boolean (0/1)
ignoreFileExtendedACL	Do not collect extended ACL information which can be time consuming, and may not be acutally used in SCAP content	Boolean (0/1)
OVAL Processing Options (Windows Only)		
onlyCollectSecurityPrinciples ThatHavePrivilegesAssigned	Only report on users/groups that have access token data assigned to them, used to save time when scanning large domain controllers	Boolean (0/1)
SCAN REPORTING OPTIONS		
allSettingsHTMLReport	Save the All Settings HTML report at the end of each scan	Boolean (0/1)
allSettingsTextReport	Save the All Settings Text report at the end of each scan	Boolean (0/1)
nonComplianceHTMLReport	Save the Non-compliance HTML report at the end of each scan	Boolean (0/1)
nonComplianceHTMLReport	Save the Non-compliance HTML report at the end of each scan	Boolean (0/1)
allSettingsSummaryHTMLReport	Save the All Settings Summary HTML report at the end of each scan	Boolean (0/1)
allSettingsSummaryTextReport	Save the All Settings Summary Text report at the end of each scan	Boolean (0/1)
nonComplianceSummaryHTMLReport	Save the Non-compliance Summary HTML report at the end of each scan	Boolean (0/1)
nonComplianceSummaryTextReport	Save the Non-compliance Summary Text report at the end of each scan	Boolean (0/1)

XML RESULTS OPTIONS		
keepXCCDFXML	Save the XCCDF XML Results at the end of each scan	Boolean (0/1)
keepOVALXML	Save the OVAL XML Results at the end of each scan	Boolean (0/1)
keepOCILXML	Save the OCIL XML Results at the end of each scan	Boolean (0/1)
keepARFXML	Save the ARF XML Results at the end of each scan	Boolean (0/1)
keepCPEXML	Save the CPE-OVAL results if CPE-OVAL results return false (not applicable to target)	Boolean (0/1)
SUMMARY VIEWER OPTIONS		
enableSummaryViewer	Enable the Summary Viewer HTML report to provide hyperlinks to all results from a scan	Boolean (0/1)
summaryViewerSort1	Set which field to sort the Summary Viewer Report by first	Case sensitive string (Session, Stream, Host)
summaryViewerSort2	Set which field to sort Summary Viewer Report by second	Case sensitive string (Session, Stream, Host)
summaryViewerSort3	Set which field to sort Summary Viewer Report by third	Case sensitive string (Session, Stream, Host)
LOGGING OPTIONS		
keepScreenLogs	Save screen logs from each application/scan session	Boolean (0/1)
debugEnabled	Save debug logs from each application/scan session	Boolean (0/1)
suppress_warnings	Don't print warnings to the error log	Boolean (0/1)
debugExcludeDateTime	Do not print date/time stamps on every line of debug, which allows for easier comparison between debug logs	Boolean (0/1)
debugTraceEnabled	Print Trace level debug, which is more than default, enable with caution	Boolean (0/1)
maxLogFileSize	Maximum size for logs (primarily debug) before creating a new file	Integer (MB)
OUTPUT OPTIONS		
sharedOptions	Save options to SCC install directory?	Integer (1 = install to shared/install directory, 0 = install to users home directory)
userDataDirectory	Path to which SCC will save results	String
userDataDirectoryValue	How 'userDataDirectory' is determined	Integer (2 = User's home directory, 3 = Running Application Directory, 4 = Custom Directory)

OUTPUT SUBDIRECTORY OPTIONS		
dirResultsLogsEnabled	Create a subdirectory called 'Logs' for saving logs	Boolean (0/1)
dirTargetNameEnabled	Create a results subdirectory based on the target hostname	Boolean (0/1)
dirXMLEnabled	Create an results subdirectory called 'XML' for saving XML results	Boolean (0/1)
dirStreamNameEnabled	Create a results subdirectory based on the content stream name	Boolean (0/1)
dirContentTypeEnabled	Create a results subdirectory based on content type (SCAP/OVAL/OCIL)	Boolean (0/1)
dirTimestampEnabled	Create a results subdirectory of the date/time of the scan	Boolean (0/1)
OUTPUT FILENAME OPTIONS		
fileTargetNameEnabled	Include the target hostname in the result filenames	Boolean (0/1)
fileSCCVersionEnabled	Include the SCC version in the result filenames	Boolean (0/1)
fileTimestampEnabled	Include scan date/timestamp in the result filenames	Boolean (0/1)
XML Validation Options		
validateContent	Perform XML schema validation before scanning	Boolean (0/1)
validateContentOnInstall	Perform XML schema when installing content	Boolean (0/1)
validateDigitalSignature	Perform XML digital signature validation on SCAP 1.2 content before scanning	Boolean (0/1)
failOnXMLDSig	Do not scan if XML digital signature validation fails	Boolean (0/1)
validateXMLResults	Perform XML schema validation on XML results generated by SCC	Boolean (0/1)
DEVELOPER OPTIONS: MISC THRESHOLDS		
maximumRecentReports	Number of recent reports (or scan sessions) to save in the Recent Reports menu	Integer
freeSpaceThreshold	Minimum amount of free space before stopping scan	Integer (MB)
validationThreshold	Maximum file size of XML input or output to perform schema validation on	Integer (MB)
patchFileModifiedThreshold	Maximum number of days old before attempting to download new SCAP 1.0 patch content	Integer (Days)
externalcmdTimeout	Number of seconds to wait for external commands to return data.	Integer (Seconds)

SSH RESULT FILE TRANSFER OPTIONS		
sshEnabled	Enable sending of results via SSH after each scan	Boolean (0/1)
deleteOnTransferReports	Delete local results after sending to server via SSH	Boolean (0/1)
htmlReportTransfer	Transfer HTML reports via SSH	Boolean (0/1)
xmlReportTransfer	Transfer XML results via SSH	Boolean (0/1)
textReportTransfer	Transfer Text based reports via SSH	Boolean (0/1)
debugLogTransfer	Transfer debug logs via SSH	Boolean (0/1)
errorLogTransfer	Transfer error logs via SSH	Boolean (0/1)
sshServer	Name of ssh server to send results to	Boolean (0/1)
sshPortNumber	Port number for SSH	Integer
sshConnectionType	SSH Connection Type	Integer (0 = username, private key and passphrase; 1 = username and password)
username	SSH Username	String
sshUserPassword	Encrypted by SCC, cannot be edited manually	String
sshPrivateKey	Full path to user's private key for SSH connections	String
sshUserKeyFile	SCC generated keyfile for use with SSH	String
sshKeyPassphrase	Encrypted by SCC, cannot be edited manually	String
sshServerDirectory	Directory on the SSH in which to send results	String
POST SCAN SCAP SUMMARY REPORTING OPTIONS		
summarySourceDirectory	Source directory for post scan SCAP summary reports	String
summaryDestinationDirectory	Destination directory for post scan SCAP summary reports	String
openSummaryDestinationDirectory	Open Windows Explorer to the directory containing the reports (Windows only)	Boolean (0/1)
computerListHistoricalHTMLReport	Generate the Computer List Historical HTML report	Boolean (0/1)
computerListHistoricalExcelReport	Generate the Computer List Historical Excel report	Boolean (0/1)
computerListHTMLReport	Generate the Computer List HTML report	Boolean (0/1)
computerListExcelReport	Generate the Computer List Excel report	Boolean (0/1)
siteSummaryHTMLReport	Generate the Site Summary HTML report	Boolean (0/1)
siteSummaryNonComplianceHTMLReport	Generate the Site Summary Non	Boolean (0/1)

	Compliance HTML report	
siteSummaryExcelReport	Generate the Site Summary Excel report	Boolean (0/1)
siteSummaryNonComplianceExcelReport	Generate the Site Summary Non Compliance Excel report	Boolean (0/1)
POST SCAN SCAP DETAILED REPORTING OPTIONS		
detailSummarySourceDirectory	Source directory for post scan SCAP Detailed reports	String
detailSummaryDestinationDirectory	Destination directory for post scan SCAP Detailed reports	String
openDetailSummaryDestinationDirectory	Open Windows Explorer to the directory containing the reports (Windows only)	Boolean (0/1)
POST SCAN OVAL DETAILED REPORTING OPTIONS		
detailSummaryOVALSourceDirectory	Source directory for post scan OVAL Detailed reports	String
detailSummaryOVALDestinationDirectory	Destination directory for post scan OVAL Detailed reports	String
openDetailSummaryOVALDestinationDirectory	Open Windows Explorer to the directory containing the reports (Windows only)	Boolean (0/1)
POST SCAN SCAP/OVAL SHARED REPORT GENERATION OPTIONS		
allSettingsHTMLReportDetailSummary	Regenerate the All Settings HTML Report	Boolean (0/1)
allSettingsTextReportDetailSummary	Regenerate the All Settings Text Report	Boolean (0/1)
nonComplianceHTMLReportDetailSummary	Regenerate the Noncompliance HTML Report	Boolean (0/1)
nonComplianceTextReportDetailSummary	Regenerate the Noncompliance Text Report	Boolean (0/1)
allSettingsSummaryHTMLReportDetailSummary	Regenerate the All Settings Summary HTML Report	Boolean (0/1)
allSettingsSummaryTextReportDetailSummary	Regenerate the All Settings Summary Text Report	Boolean (0/1)
nonComplianceSummaryHTMLReportDetailSummary	Regenerate the Noncompliance Summary HTML Report	Boolean (0/1)
nonComplianceSummaryTextReportDetailSummary	Regenerate the Noncompliance Summary Text Report	Boolean (0/1)
DEVIATION OPTIONS		
deviationsEnabled	Use of deviations is enabled	Boolean (0/1)
deviationsProfile	Allows usage of a different deviations file value of 'default' translates to 'default-deviations.xml'	String
THRESHOLD OPTIONS		
thresholdsEnabled	Enable usage of thresholds	Boolean (0/1)

thresholdsProfile	Allows usage of a different thresholds file value of 'default' translates to 'default-thresholds.xml'	String
thresholdsUnlockCode	Code generated by SCC Unlocker, to allow end users to modify thresholds	String
STANDALONE OVAL (NON-SCAP) CONTENT UPDATE OPTIONS		
ovalFileModifiedThresholdOC	Threshold for checking user specified URL's for updated standalone (not SCAP) OVAL content	Integer (Days)
useInternetOC	Enable checking Internet URL's for updated OVAL content	Boolean (0/1)
useIntranetOC	Enable checking Intranet URL's for updated OVAL content	Boolean (0/1)
intranetURLoneOC	Primary Intranet URL for downloading OVAL content	String
intranetURLtwoOC	Secondary Intranet URL for downloading OVAL content	String
internetURLoneOC	Primary Internet URL for downloading OVAL content	String
internetURLtwoOC	Secondary Internet URL for downloading OVAL content	String
CYBERSCOPE OPTIONS (SOON TO BE OBSOLETE)		
cyberscopeOrgName	Organization Name used for Cyberscope reporting	String
cyberscopeDepartment	Department Name used for Cyberscope reporting	String
cyberscopeEnclave	Enclave Name used for Cyberscope reporting	String
cyberscopeSummaryId	Whatever data is mandated by Cyberscope/FISMA	String
cyberscopeSummaryVersion	Whatever data is mandated by Cyberscope/FISMA	String
xccdfFileAgeWarning	Maximum age of XCCDF files before printing a warning	Integer (Days)
xccdfFileAgeAction	Action to perform with XCCDF older than threshold	String (Ignore/Warn/Exclude)
suppressCceErrors	Supress printing errors for XCCDF rules without CCE references	Boolean (0/1)
cyberscopeOrgPhone	(no longer used/required by cyberscope)	String
cyberscopeOrgURL	(no longer used/required by cyberscope)	String
cyberscopeOrgEmail	(no longer used/required by cyberscope)	String
cyberscopeReport	Internal variable to create cyberscope report, do not edit	Boolean (0/1)

SCC SERVICE OPTIONS (WINDOWS ONLY)		
frequency	How frequently SCC Service should run	Integer (0 = Custom, 1 = Hourly, 2 = Daily, 3 = Weekly, 4 = Monthly)
schedule	Custom schedule if 'frequency' = 0	Integer (Hours)
randomizeSSHTransfer	Delay SCC Service (and SSH transfer) by a random amount of time to prevent DDoS if numerous computers are configured with the SCC service and SSH transfer	Boolean (0/1)
randomizeValue	Max amount of time to delay starting SCC	Integer (seconds)
timeout	Programmatically calculated by SCC, do not edit	Integer
lastServiceScan	Programmatically calculated by SCC, do not edit	Integer
nextServiceScan	Programmatically calculated by SCC, do not edit	Integer
INTERNAL OPTIONS - DO NOT EDIT		
version	Version of SCC, do not edit	String
timeStamp	date/timestamp of last write to options, do not edit	Integer
expignore	Over-ride software expiration for pre-release versions	Boolean (0/1)
domainName	Internal variable used for Windows to generate a host file, do not edit	String
createNewHostFile	Internal variable used for Windows to generate a host file, do not edit	Boolean (0/1)
scap12DBFilepath	Relative path to the SCAP 1.2 content database, do not Edit	String
iaControlDBLoaded	Is the IA Control database loaded	Boolean (0/1)
iaControlDBFilepath	Relative path to the IA Control mappings database	String
nvdcceFile	Filename (no path) to the NVD CCE xml file	String
cciFile	Filename (no path) to the DISA CCI xml file	String
SCAP 1.0 PATCH CONTENT UPDATE (SOON TO BE OBSOLETE) OPTIONS		
useIntranet	Enable checking Intranet URL's for updated SCAP 1.0/1.1 OVAL patch content	Boolean (0/1)
patchContentAgeWarning	Threshold for checking user specified URL's for updated SCAP 1.0/1.1 OVAL patch content	Integer (Days)
intranetURLone	Primary Intranet URL for	String

	downloading SCAP 1.0/1.1 OVAL patch content	
intranetURLtwo	Secondary Intranet URL for downloading SCAP 1.0/1.1 OVAL patch content	String
useInternet	Enable checking Internet URL's for updated SCAP 1.0/1.1 OVAL patch content	Boolean (0/1)

5.3 Command Line Scanning Parameters

Before performing a scan via command line, it is recommended to view the configuration by the --config parameter, documented in section 5.2.

5.3.1 Scanning Parameters

Below are the parameters available for performing scans. Many of the options can be used in combination, as indicated in the usage below.

```
cscc.exe [-f <file> | -h <host>] [-o <file>][-drqx]
```

no parameters

Reviews the local computer based on the configuration settings found in options.xml. If options.xml does not exist in the installation directory, it will be created based on application defaults. The desired method for editing the options is via the --config command line parameter.

-d

Creates verbose debug logs in the Logs directory for troubleshooting purposes. Note that this option will generate a large amount of text based data (MB's to GB's) and will cause the application to run slower, so is not recommended for normal usage.

-ear

Enable all SCAP and OVAL content and run.

-isr <path>

Install, enable and conduct an analysis with a SCAP Content (1.0, 1.1, 1.2) stream from a zip file, or from a single SCAP 1.2 datastream XML file.. Specifying an XCCDF benchmark profile name after the file path will enable that profile for the given SCAP stream.

```
Example:   cscc.exe -isr <path>
```

-ivr <path>

Install, enable and conduct an analysis with a OVAL Content stream a single XML file or a zip file containing multiple xml files.

```
Example:   cscc.exe -ivr <path>
```

-u <directory path>

Configure SCC to save SCAP results and logs to the specified directory path.

Note: *Please refer to Appendix A.8 Debugging for additional information on SCC debug logs and their intended usage.*

-f <file name>

Reviews all computers specified in the file. This text file should contain one computer name per line.

```
Example: cscc.exe -f hosts.txt
```

Reviews the specified computer.

```
Example: cscc.exe -h <hostname>
```

-o <file name>

Reviews using the specified options file. If the file specified does not exist, the application will report an error that it does not exist. A new options file will not be created.

```
Example: cscc.exe -o myoptions.xml
```

-q

Reviews in quiet mode. No output will be displayed on the screen.

-r <xccdf rule id or oval definition>

Review a single Rule using the Rule ID from the XCCDF file or review a single definition from an OVAL document.

```
Example1: cscc.exe -r account_lockout_duration
Example2: cscc.exe -r oval:mil.disa.stig.adobe.reader:def:1
```

-mr <number of rules> <rule id> <rule id> ...

Review multiple rules using the Rule ID from the XCCDF file or review multiple definitions from an OVAL document.

```
Example1: cscc.exe -mr 2 account_lockout_duration
logon_as_service
Example2: cscc.exe -mr oval:mil.disa.stig.adobe.reader:def:1
oval:mil.disa.stig.adobe.reader:def:2
```

-x

Performs schema validation on all input and output XML files.

5.3.2 Command Line Examples

1. Review the local computer with customized report settings and do not display any data to the screen.

    cscc.exe -o myoptions.xml -q

2. Review several computers from a text file of hostnames with customized report settings.

    cscc.exe -f test.txt -o myoptions.xml

3. Review a single remote host 'computer1' in debug mode and validate the XML files

    cscc.exe -h computer1 -d -x

5.5 Generating Post Scan Reports from the Command Line

If a large number of files are collected on a share that is accessed via a LAN or WAN, it may be most time effective to generate the reports via command line on the server that contains the collection of files. This allows for a scheduled task to be created that can be run on a user specified time frame.

For example, if 100,000 computers are reviewed, it will likely take many hours to generate the summary reports. Ideally, this could be run during an evening a day after all of the results are created.

This functionality requires configuring a custom options.xml file with the GUI, and calling the application via command line with specific parameters. Refer to section 7 "Post Scan Report Generation" for details.

5.5.1 Post Scanning Report Generation Parameters

Below are the parameters available for creating reports after XML results have been created. All of the following options must be used individually, and are not compatible with any other parameter.

`-c <options file name>`

Generate the Cyberscope auto-feed XML report using the specified options file.

```
Example: cscc.exe -c options.xml
```

This option corresponds to the Generate Cyberscope Report feature in the GUI, which can be accessed via "Results-> Generate Cyberscope Report".

This command line feature uses all of the configuration options on the Generate Cyberscope Report form including the Source and Destination Directories.

`-s <options file name>`

Generate summary SCAP reports using the specified options file.

Example: `cscc.exe -s options.xml`

This option corresponds to the Generate Summary Reports feature in the GUI, which can be accessed via "Results-> Generate Summary SCAP Reports".

This command line feature uses all of the configuration options on the "Generate Summary SCAP Reports" form including the Source and Destination Directories along with all available reports.

This command line feature is available for generating summary reports from very large numbers of computers, which may take hours to complete. This command could be scheduled to run weekly or monthly, and have reports available the next day.

`-ts <options file name>`

Generate detailed SCAP reports using the specified options file.

Example: `cscc.exe -ts options.xml`

This option corresponds to the Generate Detailed SCAP Reports feature in the GUI, which can be accessed via Results-> Generate Detailed SCAP Reports.

This command line feature uses all of the configuration options on the Generate Detailed SCAP Reports form including the Source and Destination Directories along with all available reports.

This command line feature is available for generating detailed reports from very large numbers of computers, which may take hours to complete. This command could be scheduled to run weekly or monthly, and have reports available the next day.

`-tv <options file name>`

Generate detailed OVAL reports using the specified options file.

Example: `cscc.exe -tv options.xml`

This option corresponds to the Generate Detailed OVAL Reports feature in the GUI, which can be accessed via Results-> Generate Detailed OVAL Reports.

This command line feature uses all of the configuration options on the Generate Detailed OVAL Reports form including the Source and Destination Directories along with all available reports.

This command line feature is available for generating detailed reports from very large numbers of computers, which may take hours to complete. This command could be scheduled to run weekly or monthly, and have reports available the next day.

5.5.2 Other Parameters

Below are other informational parameters. All of the following options must be used individually, and are not compatible with any other parameter.

`-v`

Displays simple version information.

`-V`

Displays verbose version information.

`-?`

Displays help.

`--help`

Displays help.

5.5.3 Scheduling Command Line Generation of Summary Reports

The process for scheduling cscc.exe via the Windows Task Scheduler is the same as any other application, except the parameters listed above will need to be included. Below is an example:

1. Click Start -> Programs -> Accessories -> System Tools -> Scheduled Tasks.
2. Click "New".

3. Click "Browse".
4. Select the command line version of the file (Example "C:\Program Files\SCAP Compliance Checker 5.0.1\cscc.exe"
5. Choose the selected time frame (Daily, Weekly, Monthly, etc..).
6. Enter the credential for the software to run.
7. Click "Open Advanced Properties for this task when I click Finish".
8. Click "Finish".
9. In the Run line add the desired parameters after the double quotes.

```
Example: "C:\Program Files\SCAP Compliance Checker 5.0.1\cscc.exe" -
s options.xml
```

Test the scheduled task by right clicking and selecting "Run."

5.6 Multiple Computer Deployment

If the end user is automating the process of running the SCC software locally on multiple remote computers, below is the list of files that must be present for the application to run via command line.

- cscc.exe
- cscc32.exe
- cscc64.exe
- options.xml (or any custom named options file)
- "Resources" directory, subdirectories and all files

5.6.1 Collecting Resulting Files

If the end user is pushing the command line version of the software out to the target computers, and would like to collect the results in a consolidated directory for generating multi-computer summary reports, below is documentation explaining which files to copy.

A directory structure will be created in the format (depending on user preferences), such as:

```
SCC
     Results
          <Date Time Stamp>
               <SCAP>
                    <XML>
```

The XML Directory will contain the resulting ARF, OVAL and XCCDF XML files based on user preferences.

The only file required for generating the multi-computer reports is the XCCDF file, which will be in the XML directory, in the format:

*<Computer>_SCC_5.0.1_<DateTime>_**XCCDF-Results**_<Stream>.xml*

After all of the XCCDF XML files have been collected and copied to a centralized share, multi-computer summary reports can be created. Please refer to "Generating Multi-Computer Summary Reports" section of the documentation for additional information.

6. UNDERSTANDING SCAN RESULTS

6.1 Understanding Scan Reports

6.1.1 Summary Viewer Report

By default, with each scan session, a summary viewer HTML report is created which provides hyperlinks for easy browsing of the results created from that scan session. It's saved to the root of the scan session directory.

```
Ex:  SCC_Summary_Viewer_2017-01-06_112807.html
```

This report can be sorted by clicking on any column heading, or filtered by typing a hostname, content stream etc.. in the 'search' box.

6.1.2 Single Computer HTML and Text Reports

Depending on the user selected options, the following reports may be available in both HTML and/or text based formats:

REPORT	DESCRIPTION
All Settings Report	The *<Computer>_SCC_5.0.1_All-Settings_<Content Name>.html* report contains the XCCDF results in a human readable format. The report is divided into five sections: Score, System Information, Stream Information, Results and Detailed Results. The **Scores** section contains the calculated scores for the target system. The **System Information** section contains information about the target system (CPE Information), such as the host name, IP addresses, operating system, processor, memory, manufacturer, model, serial number, BIOS version, and Ethernet Interfaces. The **Content Information** section contains information about the XCCDF benchmark, such as the XCCDF filename used, status (if officially accepted content along with the date it was officially accepted), content installation date ,the profile used, the testing start and end times, and the identity of the user who ran the benchmark. The **Results** section contains the individual rule results, comprised of the CCE reference and the check title. To view the "Detailed Results" for an individual item, just click on the text. The **Detailed Results** section contains in-depth information on each rule performed in the benchmark. This section varies slightly between SCAP and standalone OVAL/OCIL, but contains fields such as Title, Result, CCE Identities, CVE Identities, severity, weight, definitions, tests, collected items
All Settings Summary Report	Contains the same information as the "All Settings Report", except excludes the Detailed Results, which allows for easier printing.
Non-Compliance	The *<Computer>_SCC_5.0.1_Non-Compliance_<XCCDF Content*

Report	*Name>.html* report contains same results in the same format as the "All Settings Report", but only includes the Failed, Error, and Unknown checks.
Non-Compliance Summary Report	Contains the same information as the "Non-Compliance Report", except excludes the Detailed results, which allows for easier printing.

6.1.3 Understanding the Result Status Information

All of the reports show the number of checks performed, and the result for each. The result types are specified by the SCAP standards and are summarized below.

RESULT	EXPLANATION
Pass	The SCC was able to correctly interpret the check in the XML content, perform the check on the target system, and all check requirements were met. Example: Password Length Requirement 12 Characters, Target Computer: 12 Characters
Fail	The SCC was able to correctly interpret the check in the XML content, perform the check on the target system, and one or more of check requirements were not met. Example: Password Length Requirement 12 Characters, Target Computer: 8 Characters
Error	The SCC was able to correctly interpret the check in the XML content, however an error occurred while performing the check. This is typically due to a configuration of the target system, or insufficient permissions of the user running the software.
Unknown	The SCC was not able to interpret the check in the XML content. This could be due to a flaw in the XML content, or an incompatibility between the SCC and the XML content such as OVAL version.
Not Applicable	The SCC was able to interpret the check in the XML content, but it was not applicable to the target system.
Not Checked	The SCC was able to interpret the check in the XML content, however the XML content did not result in any evaluation to be performed. Also, if a probe is not supported, the check will show up as Not Checked.
Not Selected	The SCC was able to interpret the check in the XML content, however the XML content instructed the SCC not to perform this check.
Total	Numeric sum of Pass, Fail, Error, Unknown, Not Applicable, Not Checked, and Not Selected.

6.1.4 Understanding Color Coding in the HTML Reports

The HTML reports have color coding to assist in understanding what failed, and why it failed.

6.1.4.1 Color Coding in the 'Results' Section

COLOR	DESCRIPTION
Blue	The overall rule passed all of the required tests. Example: "Account Lockout Duration - (CCE-2928-0) - Pass
Red	The overall rule failed one or more of the required tests. Example: "Account Lockout Duration - (CCE-2928-0) - Fail

6.1.4.2 Color Coding in the 'Detailed Results' Section for Class = Compliance

Per OVAL specifications, for compliance checks, a test result of "True = Compliant", and "False = Not Compliant".

COLOR	DESCRIPTION
Blue	The individual test result was True, or the result was False but did not cause the overall test to fail.
Red	The individual test was False and contributed to the overall rule being marked as Fail.

6.1.4.3 Color Coding in the 'Detailed Results' Section for Class = Patch

COLOR	DESCRIPTION
Blue	SCC was able to verify that the patch was installed as required in the underlying tests. Result = Pass
Red	SCC was not able to confirm that the patch was installed as required, as one or more of the underlying tests failed. Result = Fail

6.1.4.4 Color Coding in the 'Detailed Results' Section for Class = Vulnerability

Per OVAL specifications, for Compliance checks, a test result of True = Vulnerable and False = Not Vulnerable.

COLOR	DESCRIPTION
Blue	The individual test result was False (meaning not vulnerable), or the result was Pass (vulnerable) but did not cause the overall test to fail.
Red	The individual test was True (Vulnerable) and contributed to the overall rule being marked as Fail.

6.2 Navigating the Results Directory

If Results -> Open Results Directory is selected, Windows Explorer opens to the directory containing the HTML and text reports along with other files created during the review.

The Data Directory, which contains both the Results and Logs, is configurable, see "Editing Options" for details. By default the data is stored a subdirectory called "SCC" in the user's home directory, but can be configured to store results to the installation directory, or any custom directory.

The default Results directory structure is as follows, but is user configurable.

Results

The "Results" directory is the high level directory to save all XML, HTML and Text based reports.

<Date/Time Scan Session>

The Date/Time directory is created each time the Analyze Computer button is pressed, or a scan is completed via CSCC. This helps organize all scan related data for a single session.

SCC_Summary_Viewer_<Date/Time Scan Session>.html

The Summary Viewer report provides hyperlinks to all of the HTML, Text and XML based reports created from a single scan session.

<SCAP/OVAL/OCIL>

<Computer>_SCC_5.0.1_All-Settings_<Content>.html
<Computer>_SCC_5.0.1_Non-Compliance_<XCCDF Content>.html

XML

XML files (see table below)

6.2.1 Contents of the XML Directory

The XML folder contains XML output generated by SCC. This output can be XCCDF results, OVAL results and OVAL variables files. Refer to the "Editing Options" for enabling or disabling saving the XCCDF and OVAL XML files after each review.

These files are not designed to be human readable, but are intended to be read into another SCAP, XCCDF or OVAL compatible software product to provide consolidated results.

Note: *All filenames included in the table below are SCC's default result filenames*

XML FILE	DESCRIPTION

NIST ARF 1.1	The `<Computer>_SCC_5.0.1_<DateTime>_ARF_<XCCDF Content Name>.xml` file contains the ARF results in a machine readable format. This high level summary of the review including the asset information from each system and the pass/fail status of each check performed. This results file is required for SCAP 1.2 compliance.
XCCDF Results	The `<Computer>_SCC_5.0.1_<DateTime>_XCCDF-Results_<XCCDF Content Name>.xml` file contains the XCCDF results in a machine readable format. This is a high level summary of the review including the asset information from each system and the pass/fail status of each check performed.
OCIL Results	The `<Computer>_SCC_5.0.1_<DateTime>_ocil-res-Results_<XCCDF Content Name>.xml` file contains the detailed OCIL in a machine readable format. This is a detailed report pass/fail results from each OCIL patch check performed during a review. This file only exists if SCAP content contains an OCIL questionnaire.
OVAL CPE Results	The `<Computer>_SCC_5.0.1_<DateTime>_CPE-Results_<XCCDF Content Name>.xml` file contains the CPE results in a machine readable format. This contains platform information about the target system including the operating system, network interfaces and processor type.
OVAL Patch Results	The `<Computer>_SCC_5.0.1_<DateTime>_OVAL-Patch-Results_<XCCDF Content Name>.xml` file contains the detailed OVAL patch results in a machine readable format. This is a detailed report of pass/fail results from each OVAL patch check performed during a review. This file only exists if the SCAP content contained an OVAL patch file.
OVAL Results	The `<Computer>_SCC_5.0.1_<DateTime>_OVAL-Results_<XCCDF Content Name>.xml` file contains the detailed OVAL results in a machine readable format. This is a detailed report of pass/fail results from each OVAL definition performed during a review.
OVAL Variables	The `<Computer>_SCC_5.0.1_<DateTime>_OVAL-Variables_<XCCDF Content Name>.xml` file contains a list of OVAL variables in a machine readable format.

6.3 Viewing Screen, Error or Debug Logs

The directory containing SCC Logs (if any exist) can be opened in the Windows Explorer by clicking:

Results -> Open Log Directory

Depending on the user selected preferences, the following log files may be present:

6.3.1 Application Logs

Application Logs are logs that are created when the application is started, and during application execution outside of any scan (when the analyze button is pressed). Application Logs are created in the Logs\ApplicationLogs directory (unless that directory option is disabled) and then they are saved in the root of the Logs directory. The ApplicationLogs directory is only created when logs exist, so may not be created depending on user preferences.

Some of the following logs might be present, depending if screen or debug logs are enabled, or if any application errors occurred.

REPORT	DESCRIPTION
Screen Log	*SCC_5.0.1_<DateTime>_Screen_Log.txt* This option saves the analysis log printed to the "Status" screen to a text file for viewing after the review. This file is not saved by default, but can be enabled in Options.
Error Log	*SCC_5.0.1_<DateTime>_Error_Log.txt* This report contains any errors that may have occurred while SCC is running, but not during a specific scan. This also contains any errors that may have occurred during command line usage. If this file exists, and the error log does not provide enough information to resolve the issue, please contact SPAWAR and provide the error log for our analysis.
Debug Log	*SCC_5.0.1_<DateTime>_Debug_Log.txt* This option saves a large amount of additional information related to what occurred during a primary SCC operation, or when run via command line.. This option is disabled by default and should only be used when attempting to resolve errors in the application, as it will slow down the application and potentially use large amounts of disk space. Please refer to Appendix A.8 Debugging for additional information on SCC debug logs and their intended usage.

6.4.1 Scan Logs

Scan Logs are logs that are created when any SCAP/OVAL/OCIL content is used to scan a target computer. By default the logs are created in a date/timestamp 'session' directory within the Logs directory. Each time the Analyze button is pressed, a new scan log subdirectory is created. This directory name matches the same date/time session directory created in the Results directory.

REPORT	DESCRIPTION
Scan Screen Log	*SCC_5.0.1_<DateTime>_Screen_Log.txt* This option saves the analysis log printed to the "Status" screen to a text file for viewing after the review. This file is not saved by default, but can be enabled in Options.
Scan Error Log	*SCC_5.0.1_<DateTime>_scan<number>_Error_Log.txt* This report contains any errors that may have occurred during a GUI based scan. The scan<number>, such as scan001 or, scan002 corresponds to each review that is started by clicking the Analyze button. Normally this file will not exist. If this file exists, and the error log does not provide enough information to resolve the issue, please contact SPAWAR and provide the error log for our analysis.
Scan Debug Log	*SCC_5.0.1_<DateTime>_scan<number>_Debug_Log.txt* This report contains any debug that occurred during a scan. The scan<number> such as scan001, scan002 corresponds to each review that is started by clicking the Analyze button. This option saves a large amount of additional information related to what occurred during a review. This option is disabled by default and should only be used when attempting to resolve errors in the application, as it will slow down the application and potentially use large amounts of disk space. Please refer to Appendix A.8 Debugging for additional information on SCC debug logs and their intended usage.

7. RUNNING SCC AS A SERVICE

This section of the manual is only applicable to installations of SCC on Windows. Automated command line usage of SCC on Linux, Solaris and Mac OS X is possible, but requires end users to script the command line interface by methods such as cron.

Installing SCC as a service, is completely optional, and only provided to allow easier automated scanning. It is recommended to configure sending results via SSH with running SCC as a service, to automate data collection as well. Refer to the SSH section for instructions on its usage.

7.1 Installing the SCC Service

During the installation of SCC on Windows, the installer provides an option to install the SCC Service component. If this was not selected at install, re-install the software and enable this option.

7.2 Configuring the SCC Service

The SCC application has a SCC Service Configuration component available, but only if the SCC Service was installed during application install.

Start -> Programs -> SCAP Compliance Checker 5.0.1 -> SCAP Compliance Checker 5.0.1 -> Options -> Show Options -> Service Options

7.2.1 Service Status

This option displays the current status of the service. However this does not indicate that the SCC application is actively scanning the computer, just that the service itself is running.

7.2.2 Scan Scheduling

This option allows the frequency at which SCC should perform scans, based on the options specified on this form.

Last Scan: Displays the date/time of the last scan performed by SCC as a service
Next Scan: Displays the date/time of the next scheduled scan, assuming the SCC service is Enabled and running.

Below are the user configuration options for scheduling scans:

- **Daily** - SCC will scan once per day.
- **Weekly** - SCC will scan once per week.
- **Monthly** - SCC will scan once per month.
- **Custom** (Number of Hours) Enter a numeric value say N (1-1000 etc..) for the frequency to at which SCC should scan. SCC will then scan the computer every N hours.

7.2.3 Other Options

All of the remaining options available for configuration are the same as SCC's options and include Reports, File Types, Logging, SCAP Content, OVAL Content, SSH Options. Refer to 'Using the Software via GUI' for documentation for each option.

Note: *The options saved for the SCC service will inherit all configuration settings from the SCC application, but only at the time the Save Service Configuration is pressed.*

7.2.4 Directory Options, Saving Results to Home Directory

If the SCC option for saving results is set to the Users Home Directory, SCC will save results to the Local System account home directory which is normally C:\Windows\System32\config\systemprofile, so the results will be stored in C:\Windows\System32\config\systemprofile\SCC.

To change this option to another directory, just update the Directory option in the SCC GUI before saving the Service Configuration.

7.2.5 Files/processes used in the SCC Service

The following process will appear in the process table, and will be running in the background: SCC_Service.exe

Depending on the scan frequency, periodically, the command line version of SCC will also be present in the process table: cscc.exe

7.3 Update Service Configuration

7.3.1 Save Current Configuration to Service

This button saves the current configuration of SCC to the SCC service, then starts or restarts the SCC Service as needed.

7.3.1 Stop Service

This button stops and sets the startup of the SCC Service to 'Manual', effectively disabling the service. To re-enable the service, click the Save Current Configuration to Service button..

APPENDIX A - FREQUENTLY ASKED QUESTIONS

A.1 Why can't I install a DISA STIG Manual XCCDF into SCC?

Below is a common question:

> I tried to import a "Manual" STIG as a *.zip into the SCC and it gives me the following error:
>
> ```
> "Unable to find OVAL document.*.zip Please ensure that all SCAP
> streams include a valid OVAL file that is named '<stream_name>-
> oval.xml"
> ```
>
> I then tried to import a manual STIG as a *-xccdf.xml into the SCC and gives me the following error:
>
> ```
> "Error installing file, *-xccdf.xml: SCC did not find a valid
> SCAP 1.2 data-stream-collection"
> ```

Answer:

> DISA STIG "Manual"'s are not SCAP content. They contain an XCCDF XML file, with a xslt transform, meant to be viewed with Internet Explorer in order to perform a manual assessment of the system. They do not contain any OVAL xml, which is required for automation.
>
> To obtain SCAP content from DISA, download "Benchmarks" from http://iase.disa.mil/stigs/scap/Pages/index.aspx

A.2 Can I scan Linux/Solaris/HPUX/AIX from Windows or vice-versa?

No. Remote scanning is only possible from Windows to Windows, and only in the same Active Directory Domain.

A.3 How can I scan SUSE, Ubuntu or Debian etc.. with an existing SCAP benchmark?

SCAP content is designed to be applicable to a specific OS or application version, but SCC has a feature to ignore this.

GUI:

```
Options -> Show Options -> Scanning Options -> SCAP Options -> Run
all content regardless of CPE-OVAL applicability
```

CSCC

```
cscc --config -> 6. Configure Options -> Scanning Options -> 3.
[X] Run all content regardless of CPE-OVAL applicability
```

A.4 Is SCC officially SCAP validated?

Yes. SCAP Compliance Checker version 4.1.1 was officially SCAP validated on August 26, 2016 against the SCAP 1.2 standards.

SCC currently supports SCAP versions 1.0, 1.1, and 1.2.

A.5 How can I report an issue with DISA STIG SCAP content to DISA?

SCAP content (not SCC) issues can be reported by sending an email to:
disa.stig_spt@mail.mil

A.6 How can I report an issue with USGCB SCAP content to NIST?

SCAP content (not SCC) issues can be reported by sending an email to: usgcb@nist.gov

A.7 Does SCC provide any remediation functionality?

No. This software only analyzes the system, it does not modify any setting.

A.8 Is it possible to write custom SCAP content and use it with SCC?

Yes, although creating content is not a trivial process.

A.9 Where can I learn more about creating SCAP content?

http://csrc.nist.gov/publications/PubsSPs.html - (SP800-126 and SP 800-117)

http://ovalproject.github.io/ - OVAL

http://scap.nist.gov/specifications/xccdf/ - XCCDF documentation

A.10 Are there any specific tools available for creating SCAP content?

Unfortunately, no. Several prototypes were created, but in the end, the best overall tool is just a skilled software developer with a high quality XML editor.

A.11 Are there any tools available for checking content for validity/correctness?

Yes.

SCAP Content Validation Tool from NIST

http://scap.nist.gov/validation/resources.html

A.12 Can SCC run directly from a CD-ROM?

No. If you need this capability, please use SCC 4.2.

A.13 How can I use the XML result files with DOD VMS?

SCC, and all SCAP validated applications create SCAP required XML results (XCCDF and OVAL). The SCAP XML results are not directly supported by the DOD Vulnerability Management System (VMS), but can be converted to VMS format by using the DISA developed STIG Viewer. The STIG Viewer can read in XCCDF source STIG policies and XCCDF results from SCAP Validated applications.

For additional information regarding the STIG Viewer: http://iase.disa.mil/stigs/Pages/stig-viewing-guidance.aspx

A.14 How can I use RunAs (Secondary Logon) with SCC?

Background: Why would a user need to do this?

If a user is logged on a non-administrative account or to one domain and wishes to review computers in a different domain, the use of the RunAs command can allow the user to complete this task without having to logon to the computer as domain administrator of the target domain.

Option 1: Run via Start Menu Shortcut as privileged user

1. Click Start -> Programs -> SCAP Compliance Checker 5.0.1 -> then Right click on SCAP Compliance Checker.
2. Click on “RunAs”.
3. Type the "Domain\Username" and "Password", and then Click "OK".

Option 2: Run Command Prompt as a privileged user

1. Open the command prompt as another user and then run the application from the installation directory from the command prompt.

```
RunAs /env /user:domain_name\username "cmd"
```

A new command window will appear with a header of cmd (running as domain_name\username)

2. Change the directory to the installation directory.

```
c:  (or drive application is installed to)
cd\
cd "Program Files\SCAP Compliance Checker 5.0.1" (Install Folder)
```

3. Run the application

```
SCC.exe
or
CSCC.exe
```

OS Requirements:

- The Secondary Logon Service must be running.

Known Issue:

- The feature in the SCC software which opens the results directory (Results -> Open Results Directory) will not function as expected when running via RunAs. The Windows Explorer cannot be called while running from RunAs, this is a limitation of Microsoft Windows.

A.15 What type of network traffic does a remote Windows SCC scan generate?

SCC performs a variety of system calls as it attempts to perform compliance checks from the SCAP XML content. If the target computer is a remote computer, the SCC will generate network traffic to perform the checks. The volume and variety of network traffic will be dependent on the XML content, however, below is a list of various types of network traffic you can expect to see as a result of running SCC with the default USGCB SCAP content included in the SCC installer.

- ICMP Echo (ping) requests/replies
- TCP NBSS session requests
- TCP SMB AndX requests/responses
- TCP WINREG OpenKey/CloseKey requests/responses
- TCP RPC/DCOM (for WMI queries)
- HTTP GET (for WindowsUpdateAgent content)

APPENDIX B - KNOWN ISSUES

B.1 Potential out of memory crashes with very large OVAL XML content files

It is not recommended to install OVAL source content larger than 30 MB in size. When loading OVAL XML content, it's common for SCC to use 20-30 times the XML file size in RAM. This means that a 20 MB source OVAL XML file could use 400-600 MB of RAM to load and use. When memory usage goes above 1 GB, both system and SCC stability issues may occur.

Source OVAL XML files larger than 10 MB are not include in any SCAP content currently available, but it is possible to download raw OVAL files, such as the entire CIS OVAL repository that could cause stability issues with SCB.

B.2 Command prompt closes when run with UAC

With the update to cscc.exe to automatically elevate to a privileged user, if you run cscc.exe as a standard user, and pass in command line arguments that are invalid, Windows Vista/7 etc.. will spawn a new command prompt as administrator, in which cscc.exe runs. When the application closes, Windows closes this command prompt, and the end user will not be able to see the usage statement.

Example:
Running as a non-administrator:

```
cscc.exe -z
```

Windows will prompt the user with a User Account Control prompt, then open a new command prompt. Since the -z is not a valid parameter, cscc.exe will print the usage statement to the screen, however Windows will close the elevated command prompt before you are able to read it.

Workaround:

- Open the command prompt as administrator prior to running cscc.exe

B.3 Maximum directory/file length error when copying SCC results

SCC creates an organizational tree structure of the results from each scan, in order to allow the data to be easier to find by the end user. However, as the directory and file paths contain the SCAP Stream Name, this path can be very long, such as the following example:

C:\Program Files\SCAP Compliance Checker 5.0.1\Results\SCAP\LONG-COMPUTERNAME\U_Windows_7_V1R6_STIG_Benchmar\2\2011-12-23_160049\XML\LONG-COMPUTERNAME_SCC-5.0.1_2011-12-23_160049_OVAL-CPE-Results_U_Windows_7_V1R6_STIG_Benchmark.xml

The path above is 240 characters, which is allowable by the Windows OS, however if a user tries to copy the results to a network share, with a longer starting path, such as

\\somenetworkpath\some-long-sub-directory\some-other-sub-directory\SCAP Compliance Checker 5.0.1\Results\SCAP\LONG-COMPUTERNAME\U_Windows_7_V1R6_STIG_Benchmar\2\2011-12-

23_160049\XML\LONG-COMPUTERNAME_SCC-5.0.1_2011-12-23_160049_OVAL-CPE-Results_U_Windows_7_V1R6_STIG_Benchmark.xml

The new path is 290 characters long, which exceeds the limit of 260 set by Windows http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247%28v=vs.85%29.aspx#maxpath

Several workaround exist for this:

- In the Content and Options menu, on the Output Options tab you are able to reduce the folders created by SCC in the Output Subdirectory Options section and reduce the length of the filename using the Output Filename Options
- Only copy the results to a directory path that has less length than the SCC install path
- Only copy the results subdirectory that you need, such as SCAP
- Write a script to copy just the files you need without any directory structure into a flat directory. Since SCC includes the computername, date timestamp and SCAP stream name in the resulting files, the likelihood of conflicts is low.

B.4 Reviewing Domain Controllers with numerous user accounts

Domain controllers with large numbers of users and computers (several thousand), may not be able to be reviewed using the current DISA STIG SCAP content. There are several checks that require .* operations, which take a long time to process and can generate GB's of results, and likely will cause SCC to crash before completion.

As a partial workaround, we have added an OVAL processing option to prevent Access Token (User Rights) from causing SCC to crash, however it's not completely in accordance with the OVAL options, so it is not enabled by default.

Other checks may still exist in the content that perform .* operations for User accounts and SID's, and the only workaround would be to manually disable these rules in the XCCDF XML file.

B.5 Issues with WMI scanning if GPO is configured to block execution of all .bat files

SCC's remote WMI scanning requires the ability to create an execute a batch file. Without it, the scan will fail. See the Requirements section for more details.

APPENDIX C - TROUBLESHOOTING

There are several issues that can prevent the SCC from successfully reviewing a computer, especially remote reviews over a LAN or WAN connection. Below are some basic troubleshooting suggestions.

C.1 Verify Scanning and Target Computer are in the same Active Directory Domain

SCC only officially supports remote authenticated scanning of computers in the same (or trusted) domain. Certain tests require the usage of WMI calls, which only work when both computers are in the same domain. Certain content that does not require WMI may work correctly across domains, but most SCAP content such as USGCB and DISA will have several checks that will be unable to obtain information, and will error out if attempted from one Active Directory Domain to another.

If the computers are both stand-alone (not in any Active Directory Domain)

C.2 Ensure Necessary Services are Enabled and Running

Refer to Section 2 - Requirements to determine the required services depending on the scanning mode selected.

C.3 Ensure a Client Firewall is not Blocking the Registry, Shares or WMI

If a client firewall is blocking LAN/WAN access to the Remote Registry, File Shares or WMI, remote reviews with SCC will not possible. Enabling these port exceptions will vary for each firewall product. Please refer to your firewall software documentation regarding opening specific ports.

C.4 Verify Administrative Rights

This issue should only occur for a user wanting to review a computer that is not part of a domain for which that person is a domain administrator. In order to attain local administrative rights on a single remote computer, the user may need to map an administrative share or connect to the remote registry of that system.

C.5 Verify "Manage auditing and security log" User Right contains the Administrators group

On Windows Vista and later, SCC uses the auditpol.exe application to obtain the system's audit configuration. In order to run this command, the user running the software must have the User Right, "Manage auditing and security log". By system default, the Administrators group is a member of this right. However, if the security setting is modified and the Administrators group is removed, errors will be reported, any check related to the Windows 'Audit Policy' will error out.

C.6 Testing Connections

If SCC is unable to perform a remote review of a system, please perform the following tests before reporting any issues.

C.6.1 Map an Administrative Share

To map an administrative share to a target computer:

1. Right Click on My Computer.
2. Click on Map Network Drive. The Map Network Drive window will open.
3. In the Folder field, type in the drive you are wishing to access, most likely the C drive.

\\servername\C$

4. Deselect the "Reconnect at logon" option.
5. Click on Finish.
6. If prompted to enter Username and Password, do so using an account with administrative rights on that system.

C.6.2 Ensure Administrative Shares are enabled on the target computer

If the steps in C.6.1 do not allow you connect, but also do not prompt you for alternative connections, it's possible that the system has been configured to disable administrative shares.

1. On the target computer, login locally and open a command prompt
2. Type 'net share'
3. Verify that both the C$ and ADMIN$ shares appear

```
C:\>net share
Share name   Resource                        Remark
-------------------------------------------------------------
C$           C:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\Windows                      Remote Admin
The command completed successfully.
```

If either the C$ or ADMIN$ shares do not appear, refer to the following MSDN article regarding the registry values in HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareServer and HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareServer\AutoShareWks

C.6.3 Remotely Connect to a Computer's Registry

To Remotely Connect to Computer's Registry:

1. Click on Start – Run. The Run window will open.
2. Type in Regedit and click OK. The Registry Editor will open.
3. Select File – Connect Network Registry…
4. Type in the NetBIOS computer name in the window provided. Select OK.
5. If prompted to enter Username and Password, do so using an account with administrative rights on that system.

C.6.4 Testing the WMI Connection

Several checks in the USGCB SCAP content required WMI queries to verify data. If any checks are listed as error, it could be due to WMI configuration issues on the target computer. To test the WMI connection, perform the following:

1. Click Start -> Run.
2. Type mmc.exe.
3. Click File - > Add/Remove Snap-In.
4. Click the Add button.
5. Scroll Down to WMI Control and Click on it.
6. Click the Add button.
7. Click the radio button next to "Another Computer".
8. Type the computer you want to test.
9. Click Finish.
10. Click Close.
11. Click OK.
12. Right Click on WMI Control for <Computername>.
13. Click Properties.
14. If the General Tab states "Successfully Connected to: \\<Computername>, then a WMI based review should be possible.
15. If any errors are listed on this tab, the troubleshooting is outside the scope of this manual.

C.6.4.1 Microsoft WMI Links

Below are some links maintained by Microsoft related to WMI.

- Troubleshooting and Tips https://technet.microsoft.com/en-us/library/ee692772.aspx
- How to enabled DCOM: http://msdn2.microsoft.com/en-us/library/ms687298.aspx

C.6.4.2 Verify 'Restrictions for Unauthenticated RPC Clients Setting' is not set to 'Enabled: Authenticated Without Exception'

Review the following setting: Policies\Administrative Templates\System\Remote Procedure Call "Restrictions for Unauthenticated RPC Clients". This can be set to either "Not Configured" (default) or "Enabled: Authenticated". If it is set to the highest setting "Enabled: Authenticated Without Exception" we have seen instances where this will no longer allow review of a system via WMI.

C.6.5 Test DCOM connections

The easiest way to test remote DCOM connections may be to run SCC with any WuaUpdateSearcher content, and review the errorlog. Additionally, there is a DCOM testing tool available from Microsoft.

http://support.microsoft.com/kb/259011

C.6.6 Test ability to run auditpol.exe

To test run the following command, which should return back all of the audit configuration of the local computer:

```
Auditpol /backup /file:<file>
```

If this returns any error messages, SCC will not be able to check the audit configuration of the computer. In order to allow SCC or most applications to view the audit configuration, the Administrators group will need to be added back to the "Manage auditing and security log" User Right.

C.6.7 Re-scan with SCC

If all of the above tests were successful, please re-scan the target computer with SCC.

APPENDIX D – SCC AND SCAP

D.1 SCAP Validations & Capabilities

- SCAP Versions Supported
  - SCAP Version: 1.0
    - Validation Date: February 25, 2009
  - SCAP Version: 1.1
  - SCAP Version: 1.2
    - Validation Date: August 26, 2016
- SCAP Capabilities
  - Authenticated Configuration Scanner (ACS)
  - Common Vulnerability Enumeration (CVE)
  - Open Checklist Interactive Language (OCIL)

D.2 Standards Supported

STANDARD	VERSION SUPPORTED
SCAP	1.0, 1.1, and 1.2
OVAL	5.3 -> 5.11.1
OCIL	2.0
XCCDF	1.1.4 and 1.2
CPE	2.2
CCE	5.0
DOD ARF	0.41
NIST ARF	1.1
Cyberscope	DRAFT 1.0.0 Early Access Release

D.3 SCAP Implementation

SCAP (Security Content Automation Protocol) is a suite of standards used to determine the presence of vulnerabilities, patches and configuration issues on a target system. SCAP content consists of machine readable XML files that contain configuration data, checklist data and logic used to scan a system. The standards include CVE (Common Vulnerabilities and Exposures), CCE (Common Configuration Enumeration), CPE (Common Platform Enumeration), XCCDF (eXtensible Configuration Checklist Description Format), OVAL (Open Vulnerability and Assessment Language) and CVSS (Common Vulnerability Scoring System).

SCAP Compliance Checker processes SCAP content on a target system and produces HTML and text reports, XCCDF results and OVAL results. The HTML and text reports provide benchmark scores and information that a system administrator can use to make the target system more secure. The XCCDF results and OVAL results can be used by other tools in a variety of ways since they are generated using the industry standard XCCDF and OVAL results formats.

SCAP Compliance Checker reads in a SCAP stream which includes XML files written in the XCCDF, OVAL and CPE Dictionary schemas. SCAP Configuration Checker then generates XML results files using the XCCDF and OVAL results schemas. The HTML reports are generated by transforming the generated XCCDF and OVAL XML results files into human readable output. This output contains detailed scoring and results information, as well as CVE, CCE and CPE identifiers.

SCAP Compliance Checker is capable of validating SCAP streams against the industry standard XCCDF and OVAL schemas. All output generated by SCAP Configuration Checker can also be validated.

SCAP Compliance Checker was designed specifically to process SCAP content. This includes the USGCB Windows Firewall content (Windows XP, Vista and 7), the Internet Explorer 7 & 8 content, and the Windows XP, Vista and 7 operating system content for Windows, and the USGCB Red Hat Enterprise Linux 5 content for Linux.

SCAP Compliance Checker 5.0.1 implements SCAP version 1.0, 1.1 and 1.2.

D.3.1 How SCC Process SCAP 1.0/1.1 Data Streams

SCC follows the Use Case Requirements in NIST 800-126 which document the following:

COMPONENT	STREAM LOCATOR	REQUIRED/OPTIONAL
XCCDF Benchmark	xxxx-xccdf.xml	Required
OVAL Compliance	xxxx-oval.xml	Required
OVAL Patch	xxxx-patches.xml	Optional
CPE Dictionary	xxxx-cpe-dictionary.xml	Required
CPE Inventory	xxxx-cpe-oval.xml	Required

Where "xxxx" indicates the SCAP stream name, which must be consistent across all files in the SCAP Stream.

From 800-126: "The notation "xxxx" designates a locator prefix that SHALL be associated with a use case specific data source component stream.

The SCC order of operations with a SCAP stream is as follows, and the USGCB 2.0.0.0 Windows XP Stream is used as an example. SCAP Stream Name = "USGCB-Windows-XP"

1. SCC verifies if the XCCDF Benchmark, OVAL Compliance, CPE Dictionary and the CPE Inventory exist for the specified SCAP stream.

USGCB-Windows-XP-xccdf.xml

USGCB-Windows-XP-oval.xml

USGCB-Windows-XP-cpe-dictionary.xml

USGCB-Windows-XP-cpe-oval.xml

2. If all required files are present, SCC then loads the XCCDF file to gather platform information.

USGCB-Windows-XP-xccdf.xml

3. Based on the Profile that was selected in the options form, the SCC then finds the matching profile, and then checks to ensure the profile is not an abstract profile. (<Profile> element doesn't have an "abstract" attribute or the attribute is set to "false".)

united_states_government_configuration_baseline_version_2.0.0.0

4. Next the CPE Dictionary is processed. The platform element from the XCCDF is used to determine what CPE items the target system is part of.

USGCB-Windows-XP-cpe-oval.xml

USGCB-Windows-XP-cpe-dictionary.xml

5. If the content is applicable to the target computer based on the CPE OVAL tests, the XCCDF content is then traversed and loads the OVAL file and/or the OVAL patches files (from filename) and definitions are processed. The definitions that get processed come from the XCCDF rules found during the XCCDF traversal.

USGCB-Windows-XP-oval.xml

USGCB-Windows-XP-patches.xml

6. XML results are created, based on user settings in the options form of the GUI or the --config from the command line.

<Computer>_SCC_5.0.1_<Date-Time>_OVAL-CPE-Results_USGCB-Windows-XP.xml

<Computer>_SCC_5.0.1_<Date-Time>_OVAL-Patch-Results_USGCB-Windows-XP.xml

<Computer>_SCC_5.0.1_<Date-Time>_OVAL-Results_USGCB-Windows-XP.xml

<Computer>_SCC_5.0.1_<Date-Time>_OVAL-Variables_USGCB-Windows-XP.xml

<Computer>_SCC_5.0.1_<Date-Time>_XCCDF-Results_USGCB-Windows-XP.xml

7. HTML and/or text based reports are generated based on end user options

D.3.2 How SCC Process SCAP 1.2 Data Streams

SCAP 1.2 as defined in NIST 800-126 rev 2 introduces data-stream-collections, data-streams, and components which are used to combine SCAP 1.0/1.2 components into a single file. Each SCAP 1.2 stream must contain a single data-stream-collection which in turn must contain at least one data-stream and one component. A data-stream may contain dictionaries and checklists, but must contain at least one check.

Upon installation of a SCAP 1.2 stream, if the file contains multiple data-streams within the data-stream-collection SCC will create a new record in the SCAP Content options for each data-stream. The user is then able to select/de-select content based on the data-stream allowing the user to run one or more data-streams from the same data-stream-collection during any given analysis run.

The SCC order of operations with a SCAP 1.2 stream is as follows, and the USGCB 1.2.7.1 Internet Explorer 8 Stream is used as an example. SCAP 1.2 Stream Name = "scap_gov.nist_datastream_USGCB-ie8-1.2.3.1.zip".

Note: *This is the data-stream name, not the data-stream-collection name*

1. SCC verifies if the XCCDF Benchmark, OVAL Compliance, OCIL Questionnaire, CPE Dictionary and the CPE Inventory components exist for the specified SCAP stream.

scap_gov.nist_comp_USGCB-ie8-xccdf.xml

scap_gov.nist_comp_USGCB-ie8-OCIL.xml

scap_gov.nist_comp_USGCB-ie8-oval.xml

scap_gov.nist_comp_USGCB-ie8-cpe-oval.xml

scap_gov.nist_comp_USGCB-ie8-cpe-dictionary.xml

2. If all required files are present, SCC then loads the XCCDF component to gather platform information.

scap_gov.nist_comp_USGCB-ie8-xccdf.xml

3. Based on the Profile that was selected in the options form, the SCC then finds the matching profile, and then checks to ensure the profile is not an abstract profile. (<Profile> element doesn't have an "abstract" attribute or the attribute is set to "false".)

xccdf_gov.nist_profile_united_states_government_configuration_baseline_version_1.2.3.1

4. If SCC detects an OCIL Component, the user is prompted to fill out the questionnaire or skip the questions and continue analysis.

scap_gov.nist_comp_USGCB-ie8-OCIL.xml

5. Next the CPE Dictionary component is processed. The platform element from the XCCDF is used to determine what CPE items the target system is part of.

scap_gov.nist_comp_USGCB-ie8-cpe-oval.xml

scap_gov.nist_comp_USGCB-ie8-cpe-dictionary.xml

6. If the content is applicable to the target computer based on the CPE OVAL tests, the XCCDF content is then traversed and loads the OVAL file and/or the OVAL patches files (from filename) and definitions are processed. The definitions that get processed come from the XCCDF rules found during the XCCDF traversal.

scap_gov.nist_comp_USGCB-ie8-oval.xml

scap_gov.nist_comp_USGCB-ie8-patches.xml

7. XML results are created, based on user settings in the options form of the GUI or the --config from the command line. SCAP 1.2 specifies the use of the NIST Asset Reporting Format (ARF) 1.1 for results generation. SCC generates an ARF results file, but we also chose to include the old reports for our current user population.

<Computer>_SCC_5.0.1_<Date-Time>_ARF_ scap_gov.nist_datastream_USGCB-ie8-1.2.3.1.zip.xml

<Computer>_SCC_5.0.1_<Date-Time>_OCIL-Results_ scap_gov.nist_datastream_USGCB-ie8-1.2.3.1.zip.xml

<Computer>_SCC_5.0.1_<Date-Time>_OVAL-CPE-Results_ scap_gov.nist_datastream_USGCB-ie8-1.2.3.1.zip.xml

<Computer>_SCC_5.0.1_<Date-Time>_OVAL-Patch-Results_ scap_gov.nist_datastream_USGCB-ie8-1.2.3.1.zip.xml

<Computer>_SCC_5.0.1_<Date-Time>_OVAL-Results_ scap_gov.nist_datastream_USGCB-ie8-1.2.3.1.zip.xml

<Computer>_SCC_5.0.1_<Date-Time>_OVAL-Variables_ scap_gov.nist_datastream_USGCB-ie8-1.2.3.1.zip.xml

<Computer>_SCC_5.0.1_<Date-Time>_XCCDF-Results_ scap_gov.nist_datastream_USGCB-ie8-1.2.3.1.zip.xml

8. HTML and/or text based reports are generated based on end user options.

D.3.3 CVE Implementation

The CVE (Common Vulnerabilities and Exposures) standard links unique identifiers with known security vulnerabilities and/or exposures. CVE identifiers are typically found in the OVAL patch definition content of a SCAP data stream. An OVAL patch definition may contain a reference element that associates the definition with a CVE identifier. Links to various websites containing more information about the vulnerability and/or exposure may also be provided in the reference element.

When the SCAP Compliance Checker processes a SCAP data stream against a target system, any CVE identifiers associated with entities in the stream will be found and provided in the results HTML and text files. It is important to distinguish that SCC does not contain any static CVE database and only imports CVE information from the content stream.

In the SCAP Compliance Checker results HTML files, CVE identifiers can typically be found in the OVAL results HTML file for the patch content. Detailed information on each definition processed can be found in the Definitions section of the HTML file. For each definition, there is a "CVE" row that displays any CVE identifiers that are associated with the definition.

It is important to note that when SCC finds a CVE identifier, it automatically creates a link in the CVE row to the NVD (National Vulnerability Database) webpage for that particular CVE identifier. This allows the user to determine the impact that a particular CVE has based on CVSS impact metrics. This also allows the user to prioritize different vulnerabilities found by comparing vulnerability scores with each other.

CVE Specification - https://cve.mitre.org

D.3.4 CCE Implementation

The CCE (Common Configuration Enumeration) standard links unique identifiers with known system configuration issues.

When the SCAP Compliance Checker processes a SCAP data stream against a target system, any CCE identifiers associated with Rules and/or definitions in the stream will be found and provided in the results HTML files. If no CCE identifiers are found within the SCAP data stream, SCC will not provide CCE information in the result files.

CCE identifiers are typically found in the OVAL definition content and the XCCDF content of a SCAP data stream. An OVAL definition may contain a reference element that associates the definition with a CCE identifier. A link to the CCE website containing more information about the system configuration issue is also provided in the reference element. An XCCDF Rule may contain an ident element that associates the Rule with a CCE identifier.

In the SCAP Compliance Checker results HTML files, CCE identifiers can typically be found in the HTML reports. For OVAL results HTML files, detailed information on each definition processed can be found in the Definitions section of the HTML file. For each definition, there is an "Identities" row that displays any CCE identifiers that are associated with the definition, in addition to the CCE identifier.

It is important to note that CCE identifiers in the Detailed Results section of the reports, provides a link to the CCE website to allow the user to gather additional information (e.g. attack vectory, dates, etc...) regarding the configuration issue.

SCAP Compliance Checker 5.0.1 implements CCE version 5.0, however the Detailed Results section of the reports displays the CCE version 4.0 as well.

CCE 5.0 Specification - http://cce.mitre.org/

D.3.5 CPE Implementation

The CPE (Common Platform Enumeration) standard is a structured naming scheme for hardware, operating systems and applications. It allows different tools to specify names for IT platforms in a consistent way. The XCCDF file included in a typical SCAP data stream contains one or more platform elements. The platform element contains a CPE identifier that associates an XCCDF Benchmark, Rule or Group with a target platform. If the target system is not an instance of the CPE identifier specified in a platform element, then the XCCDF Benchmark, Rule, or Group associated with that platform element is not applicable to the target system and will not be processed.

In order to determine if the target system is an instance of a CPE identifier, SCAP Compliance Checker processes the CPE dictionary and the CPE OVAL content in the SCAP data stream. The CPE dictionary contains one or more CPE identifiers, each associated with an OVAL definition that resides in the CPE OVAL content. If SCAP Compliance Checker processes the OVAL definition and the definition returns a result of "true", then the target system is said to be an instance of the associated CPE identifier. A list of CPE identifiers that the target system is an instance of is compiled in this fashion from the CPE dictionary, then used when processing the XCCDF file. If the CPE identifier specified by a platform element in the XCCDF file is not in the compiled CPE instance list, then the Benchmark, Rule or Group associated with that CPE identifier is not applicable to the target system and will not be processed. Rules that are not applicable to the target system will have a result of "not applicable".

SCAP Compliance Checker 5.0.1 implements CPE version 2.3.

CPE 2.3 Specification - http://csrc.nist.gov/publications/nistir/ir7695/NISTIR-7695-CPE-Naming.pdf

D.3.6 CVSS Implementation

The CVSS (Common Vulnerability Scoring System) standard is a system used to assign scores to vulnerabilities. By assigning a score to a vulnerability, one can determine its relative severity when compared to other vulnerabilities.

In the SCAP Compliance Checker the CVE identifiers can typically be found in the security patches section of the HTML reports. For each security patch check, there is a "References" row that displays any CVE identifiers that are associated with the definition. Each CVE identifier will have a link to the NVD database webpage for that CVE. Each link can then be used to obtain the CVSS information from the National Vulnerability Database (NVD) site, including the NIST-calculated CVSS score, the full CVSS vector, and the CVSS calculator.

CVSS 2.0 Specification - www.first.org/cvss

D.3.7 ARF 1.1 Implementation

The ARF (Asset Reporting Format) is a data model to express the transport format of information about assets and the relationships between assets and reports. The standardized data model facilitates the reporting, correlating, and fusing of asset information. SCC automatically generates the results of all SCAP 1.2 data streams into the ARF 1.1 format. The file will be included in the same folder as the other XML result files.

ARF 1.1 Specification - http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7694

D.3.8 AI Implementation

The Asset Identification (AI) 1.1 specification provides a standardized model for representing and identifying assets. The specification provides the necessary constructs to uniquely identify and correlate assets based on known identifiers and/or information about the assets. SCC identifies all assets utilizing the AI 1.1 specification in the ARF 1.1. result files.

AI 1.1 Specification - http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7693

D.3.9 TMSAD Implementation

The Trusted Model for Security Automation Data (TMSAD) is a common trusted model that can be applied to specification within the security automation domain (e..g SCAP). The TMSAD is composed of recommendations on how to use existing specifications to represent signatures, hashes, key information, and identify information in the context of an XML document and permits users to establish integrity, authentication, and traceability for security automation data.

SCC implements the TMSAD by verifying digitally signed SCAP 1.2 data streams. The XML digital signature (XMLDSig) implementation is based on requirements from the TMSAD, which includes requirements from W3C (http://www.w3.org/TR/xmldsig-core), and the NIST SP800-126 (http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf).

Supported algorithms include:

- Digests: SHA1, SHA256, SHA384, SHA512
- Encryption: DSA_SHA1, RSA_SHA1, RSA_SHA256, ECDSA_SHA256
- ECDSA Named Curves: prime256v1, secp256k1, secp384r1, secp521r1
- Transforms: C14N, C14N11, EC14N (with and without comments), enveloped signature transform
- Canonicalization: C14N, C14N11, EC14N (with and without comments)

Note: *The current implementation only supports reference that point to elements within the same document (enveloped signatures)*

TMSAD 1.0 Specification - http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7802

D.3.10 XCCDF Implementation

XCCDF (Extensible Configuration Checklist Description Format) is a language used for writing security checklists and benchmarks. SCAP Compliance Checker loads XCCDF content from a SCAP stream and determines if the Rules specified by the XCCDF content are satisfied by a target system.

SCAP Compliance Checker validates XCCDF content, imports it and allows the user to select a profile from the content. Rules are automatically selected and unselected based on the profile the user selects.

The SCAP stream's CPE dictionary and its associated OVAL definitions are then processed to determine which XCCDF Rules are applicable to the target system. Rules that are found to be inapplicable to the target system based on CPE identifiers are automatically unselected.

SCAP Compliance Checker then traverses the XCCDF content, processing all selected XCCDF Rules against a target system. Scores are calculated using all of the current XCCDF scoring models including the default, flat, flat unweighted and absolute models. Additionally two custom scoring methods are calculated, the spawar-original and spawar-adjusted.

A benchmark results XML document is generated using the XCCDF Results schema. This results file is then transformed into an HTML report, along with more in depth reports generated from the SCAP stream's OVAL content. The benchmark results XML document can be imported into other tools since it uses the industry standard XCCDF Results schema.

SCAP Compliance 5.0.11 implements XCCDF version 1.1.4 and 1.2.

XCCDF 1.1.4 - http://scap.nist.gov/specifications/xccdf/index.html#resource-1.1.4
XCCDF 1.2 - http://scap.nist.gov/specifications/xccdf/index.html#resource-1.2

D.3.11 OVAL Implementation

OVAL (Open Vulnerability and Assessment Language) is a language used to standardize the transfer of security content among different tools. SCAP Compliance Checker loads OVAL content in conjunction with an XCCDF checklist and processes the OVAL definition content against a target system.

SCAP Compliance Checker is able to process all four of OVAL's schemas: the Definitions schema, the System Characteristics schema, the Results schema and the Variables schema.

The Definitions schema is used to define definitions that test a machine's state. This schema is used in SCAP streams to specify patch, vulnerability and configuration content. SCAP Compliance Checker imports OVAL Definitions files and processes the OVAL definitions against a target system.

The System Characteristics schema is used to store data collected from a system. SCAP Compliance Checker uses Object data from OVAL Definitions content and generates System Characteristics data that is later used for testing purposes. This data is stored in an XML file using the OVAL System Characteristics schema.

The Results schema takes State data from OVAL Definitions content along with System Characteristics data and produces Definition and Test results. These results are stored in an XML file that follows the OVAL Results schema. SCAP Compliance Checker then transforms this XML file and produces human readable HTML report documents.

The Variables schema is used to import external variable data into the OVAL engine during processing of an OVAL definition. SCAP Compliance Checker processes the XCCDF content of a SCAP stream and extracts any variables that need to be imported into the OVAL engine. It then creates an XML file using the OVAL Variables schema that contains these variables. The OVAL engine later uses this file during OVAL processing.

By using the industry standard OVAL schemas, SCAP Compliance Checker can share data with any tool that understands OVAL.

SCAP Compliance Checker 5.0.1 implements OVAL version 5.3 -> 5.11.2.

OVAL 5.11.1 Specification - https://github.com/OVALProject/Language

SCAP Compliance Checker 5.0.1 is also an OVAL Adopter. The OVAL Adoption Program was established by MITRE to educate vendors on best practices regarding the use and implementation OVAL, to provide vendors with an opportunity to make formal self-assertions about how their products utilize OVAL, and to help MITRE gain deeper insights into how OVAL is or could be utilized so that the standard can continue to evolve as needed by the community.

OVAL Adoption - https://oval.mitre.org/adoption/

D.3.12 OCIL Implementation

The Open Checklist Interactive Language (OCIL) defines a framework for expressing a set of questions to be presented to a user and corresponding procedures to interpret responses to these questions. SCAP Compliance Checker loads OCIL content in conjunction with an XCCDF checklist and processes the OCIL questionnaires against a target system. SCAP Compliance Checker can also process OCIL outside of a SCAP 1.1 data stream.

SCAP Compliance Checker 5.0.1 implements OCIL version 2.0

OCIL 2.0 Specification - http://scap.nist.gov/specifications/ocil/#resource-2.0

D.3.12.1 OCIL CPE Implementation

SCAP validation requirement SCAP.V.1800.1 states:

"The vendor SHALL provide instructions on how the product indicates the applicability of the imported SCAP source data stream to a target platform. Instructions SHOULD also describe how the product indicates data streams are not applicable for a target platform. This requirement is testing the use of the OCIL questionnaire associated with a CPE name via the CPE dictionary and the platform id to determine applicability of the data stream."

SCC allows the OCIL Questionnaire to be answered prior to running the CPE applicability check so that the end user does not have to answer the same questions multiple times if multiple systems are being scanned. This allows SCC to create an OCIL Results file into a temporary directory for each system. After finishing the OCIL Questionnaire and continuing the analysis, if a CPE applicability check is included in the SCAP stream, only the OCIL questionnaires deemed applicable will be included in the final ARF results file.

D.4 OVAL Probes Supported by SCC 5.0.1 for Windows

The following OVAL probes are supported in the Windows version of SCC. For probe support on other platforms, please refer to the platform specific documentation for each release of SCC.

- Apache
  - httpd
- Cisco IOS
  - global
  - interface
  - line
  - snmp
  - version
  - version55
- Independent
  - EnvironmentVariable
  - EnvironmentVariable58
  - Family
  - FileHash
  - FileHash58
  - LDAP
  - SQL
  - SQL57
  - SQLEXT (SCC specific OVAL test, was submitted to the OVAL Board for inclusion in OVAL 5.12, but hasn't been approved)
  - TextFileContent
  - TextFileContent54
  - Variable
  - XMLFileContent
- Windows
  - AccessToken
  - ActiveDirectory
  - ActiveDirectory57
  - AppCmd
  - AuditEventPolicy
  - AuditEventPolicySubCategories
  - Cmdlet
  - DnsCache
  - File
  - FileAuditedPermissions
  - FileAuditedPermissions53
  - FileEffectiveRights
  - FileEffectiveRights53
  - Group
  - Group_SID
  - Interface
  - License
  - LockoutPolicy
  - Metabase
  - NTUser
  - PasswordPolicy
  - PeHeader

- Port
- PrinterEffectiveRights
- Process
- Process58
- Registry
- RegKeyAuditedPermissions53
- RegKeyEffectiveRights
- RegKeyEffectiveRights53
- Service
- ServiceEffectiveRights
- SharedResource
- SID
- SID_SID
- SystemMetric
- UAC
- User
- User_SID55
- UserSID
- UserRight
- Volume
- WMI
- WMI57
- WuaUpdateSearcher

D.4.1 SQL Database Management System Support

SCC supports reviews against the following SQL database configurations:

DATABASE MANAGEMENT SYSTEM	WINDOWS 2003 AND LATER	SOLARIS	RED HAT ENTERPRISE LINUX	DEBIAN LINUX
Microsoft SQL Server 2000 and Later	Yes			
Oracle Database 10g and 11g, Enterprise Edition		Yes	Yes	Yes
Oracle Database 10g and 11g, Express Edition		Yes	Yes	Yes

Local review capability is available for supported Oracle Database installations while local and remote review capabilities are available for supported Microsoft SQL Server installations.

D.4.2 SCAP Content Author Note on SQL and SQL57 implementation in SCC

SCC can recognize several common representations of the SQL Server and Oracle Database versions it supports. Such representations include chronological (SQL Server: 2005, 2008, 2008 R2; Oracle DB: 10g, 11g), short numerical (SQL Server: 9.0, 10.0; Oracle DB: 10, 11), and long numerical (SQL Server: 9.00.x, 10.00.x, 10.05.x; Oracle DB: 10.1, 11.2.0.x). Declaring multiple versions in a pattern match operation (e.g. "2005|2008", "10g|11g", or ".*") will enable SCC to concurrently analyze instances from all matching and supported versions of SQL Server or Oracle Database installed on the target system.

SCC’s handling of the “connection_string” element does not treat it as a literal connection string. Rather, it is treated as a form for specifying which instances and, if reviewing a SQL Server installation, databases on the target system should be inspected. Disregarding the quotation marks, it has one required field, “server=<instance>” where <instance> is a literal instance name or a regular expression, and one optional field, “database=<database>” where <database> is a literal database name or a regular expression. When both fields are declared, they are separated by a semicolon (;). When reviewing a SQL Server installation, declaring the “server” field as “server=MSSQLServer” will enable SCC to submit database queries against the default instance. Omitting the “database” field for a SQL Server review will cause all queries to be submitted against the default database of the specified instance(s). When reviewing an Oracle Database installation, any database declaration in the “connection_string” entity will be ignored since it would not be applicable to the Oracle Database review process. Leveraging the pattern match operation of the “connection_string” element allows SCC to analyze multiple instances and multiple matching databases, where applicable, on each instance with a single SQL or SQL57 OVAL probe.

Due to SCC's dependency upon the Oracle SQL*Plus utility for conducting Oracle Database reviews, any SQL queries specified by Oracle Database specific OVAL probes are limited to a length of 257 characters.

APPENDIX E - REFERENCES & DEFINITIONS

E.1 References

DISA STIG SCAP Benchmarks
http://iase.disa.mil/stigs/scap/Pages/index.aspx

NIST USGCB (United States Government Configuration Baseline)
http://usgcb.nist.gov

SPAWAR's SCC Page
www.public.navy.mil/spawar/Atlantic/ProductsServices/Pages/SCAP.aspx

SCAP Compliance Checker SCAP 1.2 Validation Page
https://nvd.nist.gov/scap/validation/140.cfm

NIST SCAP Specifications
http://nvd.nist.gov/scap.cfm

E.2 Definitions

ACRONYM	DEFINITION
ARF	The Asset Reporting Format (ARF) is a data model to express the transport format of information about assets and the relationships between assets and reports.
CCE	Common Configuration Enumeration CCE™ provides unique identifiers to system configuration issues in order to facilitate fast and accurate correlation of configuration data across multiple information sources and tools. For example, CCE Identifiers can be used to associate checks in configuration assessment tools with statements in configuration best-practice documents and security guides, are the main identifiers used for the settings in the U.S. Federal Desktop Core Configuration (FDCC) data file downloads, and are a key component for enabling security content automation. [1]
CIS	The Center for Internet Security. Current managers of the open source project which maintains OVAL. [6]
CPE	Common Platform Enumeration CPE™ is a standardized method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets. CPE can be used as a source of information for enforcing and verifying IT management policies relating to these assets, such as vulnerability, configuration, and remediation policies. IT management tools can collect information about installed products, identify products using their CPE names, and use this standardized information to help make fully or partially automated decisions regarding the assets.[1]
CVE	Common Vulnerability Enumeration CVE® International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures. CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.[1]
DISA	Defense Information Systems Agency The Defense Information Systems Agency (DISA) is a United States Department of Defense agency that provides information technology (IT) and communications support to the President, Vice President, Secretary of Defense, the military Services, and the Combatant Commands.[2] With respect to SCC and SCAP, DISA creates and maintains SCAP content for the DISA STIGS.
MITRE	MITRE is a not-for-profit corporation, chartered to work solely in the public interest. MITRE operates multiple Federally Funded Research and Development Centers (FFRDCs).[1] With regards to SCAP, MITRE develops and maintains several standards such as CPE, CCE and CVE (and formerly OVAL).
NIST	National Institute of Standards and Technology

	NIST is a United States Government agency responsible for many government standards, including SCAP.
OCIL	Open Checklist Interactive Language The Open Checklist Interactive Language (OCIL) defines a framework for expressing a set of questions to be presented to a user and corresponding procedures to interpret responses to these questions. Although the OCIL specification was developed for use with IT security checklists, the uses of OCIL are by no means confined to IT security. Other possible use cases include research surveys, academic course exams, and instructional walkthroughs.[3]
OVAL	Open Vulnerability and Assessment Language Open Vulnerability and Assessment Language (OVAL®) is an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. OVAL includes a language used to encode system details, and an assortment of content repositories held throughout the community. The language standardizes the three main steps of the assessment process: representing configuration information of systems for testing; analyzing the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.); and reporting the results of this assessment. The repositories are collections of publicly available and open content that utilize the language.[1]
SCAP	Security Content Automation Protocol SCAP (pronounced S-CAP) consists of a suite of specifications for standardizing the format and nomenclature by which security software communicates information about software flaws and security configurations. [3] NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets; but such standards and guidelines shall not apply to national security systems.[3]
SCC	SCAP Compliance Checker SCAP Validated Authenticated Configuration Scanner developed by SPAWAR Atlantic.
SPAWAR	Space and Naval Warfare SPAWAR Systems Center Atlantic is a Department of the Navy organization. We meet our nation's demands for uninterrupted vigilance, fail-safe cybersecurity, adaptive response and engineering excellence by delivering secure, integrated and innovative solutions to many naval, joint and national agencies. [4]
STIG	Security Technical Implementation Guides The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. Since 1998, DISA Field Security Operations (FSO) has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack. [5]

USGCB	United States Government Configuration Baseline The purpose of the United States Government Configuration Baseline (USGCB) initiative is to create security configuration baselines for Information Technology products widely deployed across the federal agencies. The USGCB baseline evolved from the Federal Desktop Core Configuration mandate. The USGCB is a Federal government-wide initiative that provides guidance to agencies on what should be done to improve and maintain an effective configuration settings focusing primarily on security. [3]
XCCDF	The Extensible Configuration Checklist Description Format XCCDF is a specification language for writing security checklists, benchmarks, and related kinds of documents. An XCCDF document represents a structured collection of security configuration rules for some set of target systems. The specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring. The specification also defines a data model and format for storing results of benchmark compliance testing. The intent of XCCDF is to provide a uniform foundation for expression of security checklists, benchmarks, and other configuration guidance, and thereby foster more widespread application of good security practices.
XML	Extensible Markup Language (XML) is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. [2]

[1] - http://www.mitre.org
[2] - http://www.wikipedia.org
[3] - http://www.nist.gov
[4] - http://www.public.navy.mil
[5] - http://iase.disa.mil
[6] - http://cisecurity.org

APPENDIX F - LICENSES

F.1 End User License Agreement

Any usage or distribution of this software outside of the U.S. Federal Government shall be reviewed by the agency distributing the software to ensure the distribution complies with the government purpose rights listed below, and is in the best interest of the U.S. Federal Government.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

The U.S. Federal Government has at least "government purpose rights" for this computer software under DFARS 252.227-7014. This computer software is to be used only for a "government purpose" as generally defined in DFARS 252.227-7014, and specifically defined below.

The U.S Federal Government's rights to use, modify, reproduce, release, perform, display, or disclose this software are restricted by paragraph (b)(2) of the Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation. Any reproduction of the software or portions thereof marked with this legend must also reproduce the markings.

This software is designed to review computer security settings and can be installed on any U.S. Federal Government computer or any computer that is mandated to comply with U.S. Federal Government security regulations such as OMB M-08-22, FISMA, HIPPA, NIST FDCC, NIST USGCB, DISA STIGs and IRS.

The U.S Federal Government purpose in distributing this software is to increase computer security and awareness for U.S entities interfacing with the U.S Federal Government.

APPENDIX G - TECHNICAL SUPPORT

Technical support is available if a support contract has been setup between your agency and SPAWAR Atlantic. Please contact your management chain regarding any specific methods for reporting technical issues, and to determine if there is a support contract in place for your agency.

G.1 Point of Contact

To contact SPAWAR directly, please email: ssc_lant-scc@navy.mil

G.2 Software Releases

Users who have contacted SPAWAR at the email address listed above will be notified of software releases via email. Additionally, the latest official release information can be obtained from the following SPAWAR website:

www.public.navy.mil/spawar/Atlantic/ProductsServices/Pages/SCAP.aspx

G.2.1 DISA Hosted Download for DoD users

Department of Defense (DoD) users with a valid Common Access Card (CAC), can download the software directly from the following location:

http://iase.disa.mil/stigs/scap/index.html

Then click on "SCAP Tools", and click on the platform specific release of SCC to download.

G.2.2 OMB Hosted Download for Federal Government users

For US Government Employees and contractors, the software can be obtained via the Office of Management and Budget (OMB) hosted MAX.omb.gov website. Users will be required to self-activate an account in order to obtain the files.

After registration, the software can be downloaded from:
https://max.omb.gov/community/x/KYRhKg

G.3 Credits

The development of SCC was originally funded by the Internal Revenue Service (IRS), with later funding from the National Security Agency (NSA), and is currently funded by Defense Information Systems Agency (DISA).

Special thanks to all of our Beta testers, and anyone who has sent us suggestions on the application!